Konstruierbarkeit mit Origami im Vergleich zu Zirkel und Lineal mit Winkeldreiteilung

Und Torsionspunkte der Ordnung 2^n und $2^n \cdot 3$ auf elliptischen Kurven als Anwendung der Konstruierbarkeit mit Origami

Bachelor-Thesis von Patrick Holzer

September 2014

TECHNISCHE UNIVERSITÄT DARMSTADT

Fachbereich Mathematik
Arbeitsgruppe Algebra

Konstruierbarkeit mit Origami im Vergleich zu Zirkel und Lineal mit Winkeldreiteilung
Und Torsionspunkte der Ordnung 2^n und $2^n \cdot 3$ auf elliptischen Kurven als Anwendung der Konstruierbarkeit mit Origami

Vorgelegte Bachelor-Thesis von Patrick Holzer

1. Gutachten: Prof. Dr. Philipp Habegger
2. Gutachten: M.Sc. Stefan Schmid

Tag der Einreichung:

Erklärung zur Bachelor-Thesis

Hiermit versichere ich, die vorliegende Bachelor-Thesis ohne Hilfe Dritter nur mit den angegebenen Quellen und Hilfsmitteln angefertigt zu haben. Alle Stellen, die aus Quellen entnommen wurden, sind als solche kenntlich gemacht. Diese Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.

Darmstadt, den 28. September 2014

(Patrick Holzer)

Danksagungen

Einen besonderen Dank möchte ich meinem Betreuer Herrn Prof. Dr. Habegger aussprechen, der dieses wunderbare Thema vorgeschlagen hat und meine vorhandenen Fragen ausführlich beantworten konnte. Vielen Dank für Ihre ausgiebige und wertvolle Unterstützung.
Daneben gilt mein außerordentlicher Dank Johanna Klein, für die tolle Zeichnung des Origami-Schwans (Titelseite), das aufwendige Korrekturlesen und die Unterstützung bei der Erstellung dieser Arbeit.
Auch meiner Lerngruppe bestehend aus Sabrina Pauli, Jan-Philipp Eisenbach und Florian Lang sowie meiner Schwester Katrin Holzer danke ich für das fleißige Korrekturlesen. Ohne euch alle wären mir sehr viele Fehler verborgen geblieben.
Nicht zuletzt möchte ich meinen Eltern für die ganze Unterstützung während meiner Studienzeit danken.

Inhaltsverzeichnis

1 Einleitung

1.1 Zusammenfassung

Die vorliegende Arbeit ist im Wesentlichen in drei Teile gegliedert: Nach einer kurzen Wiederholung algebraischer Grundlagen befassen wir uns mit der Konstruierbarkeit mit Zirkel und Lineal. Dabei arbeiten wir die kanonischen Resultate heraus, die inzwischen gut studiert und weitläufig bekannt sind. Im zweiten und wichtigsten Abschnitt beschäftigen wir uns mit der Konstruierbarkeit mit Origami und geben viele zu Zirkel und Lineal ähnliche Resultate an. Es stellt sich heraus, dass die Menge der mit Origami konstruierbaren Zahlen die Menge der mit Zirkel und Lineal konstruierbaren Zahlen derart erweitert, dass wir zusätzlich komplexe dritte Wurzeln konstruieren können. Dies motiviert die im Anschluss bearbeitete Frage, ob Konstruierbarkeit mit Origami äquivalent zur Konstruierbarkeit mit Zirkel und Lineal mit Winkeldreiteilung ist. Im letzten Teil dieser Arbeit zeigen wir, dass alle Torsionspunkte der Ordnung 2 und 3 einer elliptischen Kurve, welche über dem Körper der Origami konstruierbaren Zahlen definiert ist, mit Origami konstruierbar sind.

1.2 Motivation

Konstruktionen mit Zirkel und Lineal sind ein elementarer Bestandteil der Mathematik und haben eine weitreichende Vergangenheit. Die Theorie darüber ist heutzutage sehr gut erforscht, nicht zuletzt dank den modernen Mittel, die uns die Algebra bietet. Die Theorie der Konstruierbarkeit mit Origami ist dagegen vergleichsweise jung - das jüngste Axiom der Origami Konstruierbarkeit stammt aus dem Jahre 2003 und wurde von Koshiro Hatori entdeckt (alle Axiome tauchten bereits in einer früheren Arbeit von Jacques Justin auf, sie wurden jedoch schlichtweg von vielen Mathematikern übersehen, siehe [Lan]). Eine nähere Untersuchung der Konstruierbarkeit mit Origami scheint daher interessant, da sich herausstellt, dass Origami mehr Konstruktionen zulässt als Zirkel und Lineal, mit welchen man letztendlich nur Quadratwurzeln konstruieren kann, d.h. man kann nur Gleichungen zweiten Grades $X^2 + aX + b = 0$ lösen. Mit Origami hingegen sind Gleichungen bis vierten Grades $X^4 + aX^3 + bX^2 + cX + d = 0$ lösbar, wodurch sich einige wichtige Unterschiede ergeben. So sind z.B. von den drei antiken Problem - das delische Problem, Winkeldreiteilung und die Quadratur des Kreises - die ersten beiden mit Origami lösbar, ganz im Gegensatz zur Konstruierbarkeit mit Zirkel und Lineal, mit welcher keines der drei Probleme im Allgemeinen lösbar ist. Dies alles wirft aber die Frage auf, um welche Konstruktionen Origami denn nun die Konstruktionen mit Zirkel und Lineal erweitert. Es wird sich herausstellen, dass lediglich die Konstruierbarkeit der komplexen dritten Wurzeln hinzu kommt. Komplexe dritte Wurzeln zu konstruieren besteht dabei aus zwei Teilkonstruktionen: Die Winkeldreiteilung und die Konstruktion einer reellen dritten Wurzel. Ein Hauptresultat dieser Arbeit wird deswegen sein, zu zeigen, dass das Hinzufügen der Winkeldreiteilung zur Konstruierbarkeit mit Zirkel und Lineal nicht reicht, um alle mit Origami konstruierbaren Zahlen zu erhalten.
Am Ende dieser Arbeit wollen wir die Theorie der Konstruierbarkeit mit Origami an einem Beispiel anwenden, indem wir zeigen, dass die 2- und 3- Torsionspunkte auf elliptischen Kurven (welche über dem Körper der Origami konstruierbaren Zahlen definiert sind) mit Origami konstruierbar sind. Elliptische Kurven spielen eine bedeutende Rolle in der modernen Kryptographie, dies motiviert die Verknüpfung dieser beiden Gebiete.

2 Grundlagen

In diesem Kapitel werden grundlegende Sätze und Definitionen der Algebra wiederholt und zusammengefasst, die wir in dieser Arbeit benötigen werden. Dies ist jedoch eher als eine Zusammenfassung und weniger als eine Einführung zu verstehen, d.h. wir werden keine Beweise angeben, sondern verweisen zum Studium auf Standardwerke wie beispielsweise [Bos09], [KM13] oder [JS06]. Anschließend werden die drei antiken Probleme vorgestellt, deren Lösbarkeit mit Zirkel und Lineal oder Origami wir später untersuchen wollen.

2.1 Notationen

Mit $\mathbb{N} = \{1, 2, 3, ...\}$ bezeichnen wir die Menge der natürlichen Zahlen beginnend bei 1, wollen wir 0 mit einschließen, so schreiben wir $\mathbb{N}_0$. Die Menge aller reellen Zahlen echt größer 0 bezeichnen wir mit $\mathbb{R}_{>0}$. Für die Teilmengenbeziehung werden wir immer "$\subseteq$" schreiben, wollen wir Gleichheit ausschließen, so benutzen wir die Notation "$\subsetneq$". In den Abbildungen notieren wir ● bzw. ○ für gegebene bzw. konstruierte Punkte. Als Gerade bezeichnen wir eine Teilmenge von $\mathbb{C}$ der Form $g = \{z \in \mathbb{C} | a + t \cdot (b - a), t \in \mathbb{R}\}$, wobei $a, b \in \mathbb{C}$ mit $a \neq b$ ist. Analog dazu ist ein Kreis um a durch b definiert durch $k = \{z \in \mathbb{C} \mid |z-a| = |b-a|\}$. Als "x-Achse" bzw. "y-Achse" bezeichnen wir $\mathbb{R}$ bzw. $i \cdot \mathbb{R} = \{i \cdot r \in \mathbb{C} | r \in \mathbb{R}\}$. Geraden werden wir manchmal auch einfach durch ihre definierende Gleichung in der Form $g(t) = a + t \cdot (b-a)$ angeben.

2.2 Definitionen und Sätze über Gruppen

Wir übernehmen die übliche Notation für Gruppen, z.B. bezeichnet $[G : H]$ den Index einer Untergruppe $H \subseteq G$ in G, weiter schreiben wir $H \trianglelefteq G$, falls H ein Normalteiler von G ist.

Satz 2.2.1. *Sei $p \in \mathbb{N}$ eine Primzahl und G eine p-Gruppe der Ordnung p^k für ein $k \in \mathbb{N}_0$. Dann ist G auflösbar, d.h. es existiert eine aufsteigende Kette von Untergruppen*

$$\{1\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_k = G$$

mit $[G_{j+1} : G_j] = p$ und $G_j \trianglelefteq G_{j+1}$ für $j = 0, ..., k-1$.

Folgendes Resultat verschärft den vorigen Satz, es wurde durch W. Burnside erstmals bewiesen und trägt daher auch dessen Namen, für einen Beweis siehe [Bur04].

Satz 2.2.2 (Burnside)**.** *Seien $p, q \in \mathbb{N}$ Primzahlen und G eine Gruppe der Ordnung $p^\alpha q^\beta$ mit $\alpha, \beta \in \mathbb{N}_0$. Dann ist G auflösbar, d.h. es existiert eine aufsteigende Kette von Untergruppen*

$$\{1\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_k = G$$

mit $[G_{j+1} : G_j] \in \{p, q\}$ und $G_j \trianglelefteq G_{j+1}$ für $j = 0, ..., k-1$

2.3 Definitionen und Sätze über Körper

Auch hier übernehmen wir die übliche Notation für Körper, beispielsweise bezeichnen wir mit $[L : K]$ den Grad der Körpererweiterung L/K. Die Charakteristik eines Körpers L bezeichnen wir mit $char(L)$. Ein K-Homomorphismus zwischen zwei Körpererweiterungen L_1/K und L_2/K ist ein (Körper-) Homomorphismus $\varphi : L_1 \to L_2$ mit $\varphi|_K = id_K$. Für eine Galoiserweiterung L/K bezeichnet $\mathrm{Gal}(L/K)$ die zugehörige Galoisgruppe.

Lemma 2.3.1. *Jede endliche Körpererweiterung L/K ist algebraisch.*

Satz 2.3.2. *Falls $char(K) = 0$, so ist jede algebraische Körpererweiterung L/K separabel.*

Definition/Satz 2.3.3 ([KM13, Satz 24.13])**.** *Sei L/K eine algebraische Körpererweiterung, dann ist L/K genau dann normal, wenn jedes irreduzible Polynom aus $K[X]$, welches eine Nullstelle in L besitzt, über L in Linearfaktoren zerfällt.*

Satz 2.3.4. *Sei L/K eine Körpererweiterung, und $\alpha \in L$ algebraisch über K. Dann gilt $K(\alpha) = K[\alpha]$.*

Satz 2.3.5. *Seien L/M und M/K Körpererweiterungen, dann sind L/M und M/K genau dann algebraische Körpererweiterungen, wenn L/K algebraisch ist.*

Satz 2.3.6 (Irreduzibilitätskriterium von Eisenstein)**.** *Sei R ein faktorieller Ring (mit Eins) mit Quotientenkörper $Q = Quot(R)$ und $P(X) = \sum_{i=0}^{n} a_i X^i \in R[X] \backslash R$. Gilt $p \nmid a_n$, $p | a_i$ für $i = 0, ..., n-1$ und $p^2 \nmid a_0$ für ein Primelement $p \in R$, dann ist $P(X)$ irreduzibel in $Q[X]$.*

Satz 2.3.7. *Sei L/K eine Körpererweiterung und $a \in L$ algebraisch über K. Dann gilt $[K(a) : K] = grad(m_{a,K})$, wobei $m_{a,K}$ das Minimalpolynom von a über K bezeichnet.*

Für den nächsten Satz verweisen wir explizit auf [Bos09, Kap. 3.5, Satz 7].

Satz 2.3.8 (Normale Hülle)**.** *Sei L/K eine algebraische Körpererweiterung. Dann gilt:*

i) Es existiert eine algebraische Körpererweiterung M/L mit der Eigenschaft, dass M/K normal ist.

ii) Sei M/L eine algebraische Körpererweiterung, so dass M/K normal ist, und sei weiter $G := \{\sigma : L \to M | \sigma$ ist K-Homomorphismus$\}$. Dann ist mit $L' := K(\{\sigma(L) | \sigma \in G\})$ auch L'/L eine algebraische Körpererweiterung, sodass L'/K normal ist (L' wird auch als **normale Hülle** *bezeichnet).*

Satz 2.3.9. *Sei L/K eine Galoiserweiterung und $G := Gal(L/K)$ die zugehörige Galoisgruppe sowie $H \subseteq G$ eine Untergruppe von G. Dann ist $L^H = \{z \in L | \sigma(z) = z$ für alle $\sigma \in H\}$ ein Zwischenkörper von L/K und es gilt $[G : H] = [L^H : K]$.*

Satz 2.3.10. *Sei ξ_n eine primitive n-te Einheitswurzel, dann gilt:*

$$[\mathbb{Q}(\xi_n) : \mathbb{Q}] = \varphi(n),$$

wobei $\varphi : \mathbb{N} \to \mathbb{N}$ die Eulersche Phi-Funktion bezeichnet.

Der folgende Satz liefert uns eine Formel der Nullstellen eines allgemeinen Polynoms dritten Grades, siehe [KM13, Satz 31.8].

Satz 2.3.11 (Cardanosche Formel)**.** *Sei $P(X) \in \mathbb{C}[X]$ mit $P(X) = X^3 + t_1 X^2 + t_2 X + t_3$ gegeben. Die Nullstellen von $P(X)$ sind gegeben durch*

$$v_1 = -\frac{t_1}{3} + a' + b', \quad v_2 = -\frac{t_1}{3} + \epsilon^2 a' + \epsilon b', \quad v_3 = -\frac{t_1}{3} + \epsilon a' + \epsilon^2 b',$$

dabei bezeichnet

$$a' = \sqrt[3]{-\frac{q}{2} + \frac{1}{6\sqrt{3}}\sqrt{-D_Q}}, \; b' = \sqrt[3]{-\frac{q}{2} - \frac{1}{6\sqrt{3}}\sqrt{-D_Q}}$$

mit $D_Q = -27t_3^3 - 4t_2^3 + t_1^2 t_2^2 - 4t_1^3 t_3 + 18 t_1 t_2 t_3$, $q = t_3 - \frac{1}{3} t_1 t_2 + \frac{2}{27} t_1^3$ und $\epsilon = e^{2\pi i/3}$. Die dritte Wurzel a' kann dabei beliebig gewählt werden, während b' folgende Gleichung erfüllen muss:

$$3a'b' = \frac{1}{3} t_1^2 - t_2$$

2.4 Die drei antiken Problemstellungen

Die folgenden drei Problemstellungen werden wir in späteren Kapiteln auf Lösbarkeit mit Zirkel und Lineal bzw. Origami untersuchen. Die einzelnen Probleme lassen sich dabei immer auf die Konstruierbarkeit einzelner Zahlen zurückführen, indem man die Zeichenebene mit $\mathbb{C}$ identifiziert und $0, 1$ als gegebene Startpunkte voraussetzt.

Die antiken Probleme 2.4.1.

(1) ***Das delische Problem**: Ist es möglich, aus einem gegebenen Würfel einen Würfel mit doppeltem Volumen zu konstruieren? (Äquivalent dazu ist die Frage, ob $\sqrt[3]{2}$ konstruierbar ist).*

(2) ***Winkeldreiteilung**: Ist es möglich, aus zwei nicht parallelen Geraden eine dritte Gerade zu konstruieren, die den Winkel der anderen beiden dreiteilt? (Analog zur Frage, ob aus $0, 1, e^{i\varphi}$ auch $e^{i\varphi/3}$ konstruierbar ist).*

(3) ***Die Quadratur des Kreises**: Lässt sich aus einem gegebenen Kreis ein flächengleiches Quadrat konstruieren? (Äquivalent zur Konstruierbarkeit von $\sqrt{\pi}$).*

Bemerkung 2.4.2.

- *Die Äquivalenz in (1) folgt daraus, dass die Seitenlänge s eines Würfels mit doppeltem Volumen des Einheitswürfels (Seitenlänge 1) die Bedingung $s^3 = 2 \cdot 1^3 = 2$ erfüllt.*
- *Die Äquivalenz in (2) ist offensichtlich, wenn man mit den Regeln der Konstruierbarkeit mit Zirkel und Lineal oder Origami vertraut ist. Dies folgt in den nächsten Kapiteln.*
- *Der Kreis mit Radius 1 hat den Flächeninhalt π, ein flächengleiches Quadrat hat demnach die Seitenlänge $\sqrt{\pi}$. Dies begründet die Äquivalenz in (3).*

Die Quadratur des Kreises ist mit Sicherheit das bekannteste Problem dieser drei Problemstellungen, daher gab es schon oft vermeintliche "Lösungen", wie die Quadratur des Kreises alleine mit Zirkel und Lineal gelingen kann. Wir werden jedoch später zeigen, dass dies unmöglich ist. Sogar in der Umgangssprache hat sich inzwischen die "Quadratur des Kreises" als Redewendung für ein unlösbares Problem eingebürgert (für eine kurze geschichtliche Einordnung siehe [Mey92]).

3 Konstruierbarkeit mit Zirkel und Lineal

3.1 Überblick

In diesem Kapitel wird es darum gehen, Konstruierbarkeit mit Zirkel und Lineal in einen exakten mathematischen Rahmen zu fassen, sodass wir mit Mitteln der Algebra und insbesondere der Galoistheorie klären können, welche der antiken Probleme mit Zirkel und Lineal lösbar sind und welche nicht. Dabei halten wir uns ungefähr an die Vorgehensweise aus [KM13]. Unsere Zeichenebene werden wir dabei mit den komplexen Zahlen $\mathbb{C}$ identifizieren, als gegebene Startpunkte wählen wir $\{0, 1\}$. Weiter werden wir elementare geometrische Sätze wie beispielsweise den Strahlensatz benutzen, die wir als bekannt voraussetzen.

3.2 Konstruktionen mit Zirkel und Lineal

Definition (nach [KM13, 22.1.1])**.** *Sei $K \subseteq \mathbb{C}$ mit $0, 1 \in K$ gegeben. Die Menge $K_n \subseteq \mathbb{C}$ der in $n \in \mathbb{N}_0$ Schritten aus K mit Zirkel und Lineal konstruierbaren Zahlen ist wie folgt rekursiv definiert:*

$$K_n := \begin{cases} K, & \text{falls } n = 0 \\ K_{n-1} \cup S_{g,g}(K_{n-1}) \cup S_{g,k}(K_{n-1}) \cup S_{k,k}(K_{n-1}), & \text{sonst} \end{cases}$$

Dabei bezeichnet

- $S_{g,g}(K_{n-1})$ die Menge aller Schnittpunkte zweier nicht paralleler Geraden, die jeweils durch mindestens zwei verschiedene Punkte aus K_{n-1} verlaufen.
- $S_{g,k}(K_{n-1})$ die Menge aller Schnittpunkte von Geraden mit Kreisen, wobei die Geraden durch mindestens zwei verschiedene Punkte aus K_{n-1} verlaufen und die Mittelpunkte sowie ein weiter Punkt auf den Kreisen ebenfalls in K_{n-1} liegen müssen.
- $S_{k,k}(K_{n-1})$ die Menge aller Schnittpunkte zweier verschiedener Kreise, deren Mittelpunkt sowie ein weiterer Punkt auf jedem Kreis in K_{n-1} liegen.

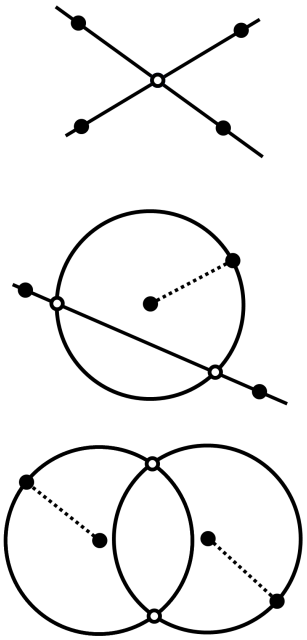


Abbildung 3.1: Mögliche Konstruktionen

Die Menge $\mathscr{Z}(K) \subseteq \mathbb{C}$ aller aus K mit Zirkel und Lineal konstruierbaren Zahlen ist damit definiert als

$$\mathscr{Z}(K) := \bigcup_{n=0}^{\infty} K_n.$$

Im Folgenden werden wir immer voraussetzen, dass $0, 1 \in K \subseteq \mathbb{C}$ gilt. Statt "$z \in \mathscr{Z}(K)$" werden wir auch häufig "$z \in \mathbb{C}$ ist konstruierbar" schreiben. Eine Gerade bzw. einen Kreis nennen wir konstruierbar, falls zwei verschiedene Punkte auf der Geraden bzw. ein Punkt auf dem Kreis und dessen Mittelpunkt konstruierbar sind. Wir werden nun noch ein paar elementare Konstruktionen angeben, die sich für spätere Beweise als nützlich erweisen werden.

Beispiel 3.2.1. *Seien $a, b, c \in \mathbb{C}$ mit $a \neq b$, dann lässt sich Folgendes konstruieren:*

i) *Die Mittelsenkrechte der beiden Punkte a, b auf deren Verbindungsgerade (und damit auch der Mittelpunkt von a und b).*

ii) *Die Senkrechte auf der Verbindungsgerade von a und b, welche durch c verläuft.*

iii) *Die zur Verbindungsgeraden von a und b parallele Gerade durch c.*

iv) *Falls die drei Punkte a, b, c nicht auf einer Geraden liegen, sind die Winkelhalbierenden der beiden Geraden durch a, b und a, c konstruierbar.*

v) *Der Kreis mit Radius $r = |b - a|$ um c ist konstruierbar (und damit auch r).*

vi) *Es gilt $\mathbb{Z} \subseteq \mathscr{Z}(K)$.*

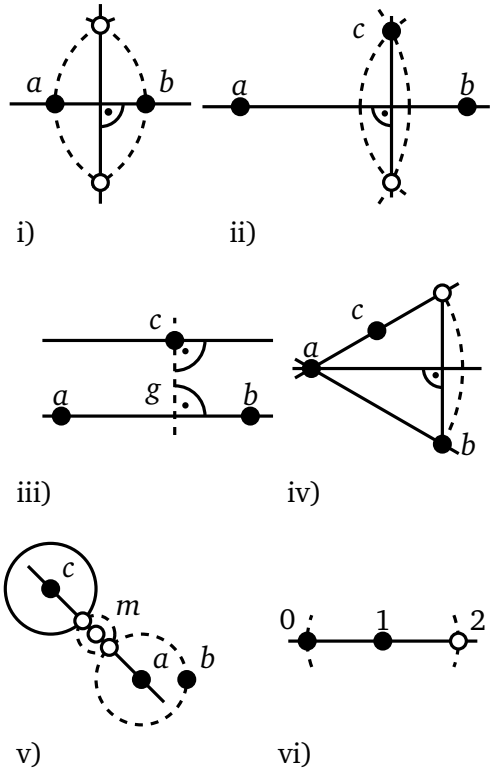


Abbildung 3.2: Konstruktionen mit Zirkel und Lineal

Beweis. Wir geben eine kurze Erläuterung zu den einzelnen Konstruktionen und Aussagen:

i) Da a und b verschieden sind, haben die beiden Kreise um a und b mit Radius $r := |b-a|$ zwei verschiedene Schnittpunkte. Die Gerade durch diese beiden Punkte ist die gesuchte Mittelsenkrechte. Der Schnittpunkt der Mittelsenkrechte und der Gerade ist der Mittelpunkt von a und b.

ii) Falls a, b und c nicht auf einer Geraden liegen, so kann man die gesuchte Senkrechte wie in der Abbildung (3.2,ii)) konstruieren. Dazu werden wieder zwei Kreise konstruiert, deren Mittelpunkte a und b und deren Radien $r_1 := |c - a|$ und $r_2 := |c - b|$ sind. Da sich die beiden Kreise somit in mindestens einem Punkt schneiden, aber ungleich sind und der Schnittpunkt c nicht auf der Verbindungsgeraden zwischen a und b liegt, müssen sich die beiden Kreise in genau einem weiteren Punkt schneiden. Die Gerade durch diese beiden Schnittpunkte ist die gesuchte Gerade durch c.

   Liegen die drei Punkte auf einer Geraden, so gilt entweder $a \neq c$ oder $b \neq c$, o.B.d.A. $b \neq c$. Spiegeln wir den Punkt b an c (und nennen diesen Punkt b') wie in Abbildung (3.2,vi)) und bilden dann die Mittelsenkrechte von b' und b, dann ist c der Mittelpunkt dieser beiden Punkte und die nach *i)* konstruierbare Mittelsenkrechte von b und b' ist die gesuchte Gerade durch c.

iii) Liegen die drei Punkte a, b und c auf einer Geraden, so sind wir fertig. Ansonsten können wir nach *ii)* die auf der Verbindungsgeraden von a und b senkrecht stehende Gerade g konstruieren, die durch c verläuft. Nun können wir wieder nach *ii)* die zu g senkrecht stehende Gerade durch c bilden, diese ist dann unsere gesuchte Gerade.

iv) Wir bilden den Kreis um a mit Radius $r := |b-a|$. Den Schnittpunkt dieses Kreises mit der Geraden durch a und c nennen wir b'. Die Mittelsenkrechte von b und b' ist eine Winkelhalbierende der Geraden durch a und b und der Geraden durch a und c.

v) Gilt $a = c$ oder $b = c$, so können wir den Kreis per Definition konstruieren.

Sind a, b, c paarweise verschieden, so lässt sich der Kreis wie in Abbildung (3.2,v)) bilden: Im ersten Schritt konstruiert man den Schnittpunkt des Kreises um den Punkt a mit Radius $r = |b-a|$ mit der Geraden durch a und c. Falls dieser Schnittpunkt nicht $m := \frac{a+b}{2}$ ist, so bildet man einen Kreis um m, der durch diesen Punkt verläuft und man erhält somit einen weiteren Punkt auf der Geraden. Im letzten Schritt konstruiert man den Kreis um c durch diesen Punkt (bzw. m, falls der Schnittpunkt im vorigen Schritt m war), dieser hat gerade nach Konstruktion den Radius $r = |b-a|$, somit ist dies der gewünschte Kreis. Die Zahl r können wir somit als Schnittpunkt der x-Achse mit dem Kreis um 0 mit Radius r konstruieren.

vi) Nach Voraussetzung gilt $0, 1 \in \mathscr{Z}(K)$. Die Zahl 2 lässt sich wie in Abbildung (3.2,vi)) durch Spiegeln von 0 an 1 konstruieren. Induktiv erhalten wir damit $\mathbb{N}_0 \subseteq \mathscr{Z}(K)$ und durch nochmaliges Spiegeln an 0 insgesamt $\mathbb{Z} \subseteq \mathscr{Z}(K)$.

□

3.3 Eigenschaften und Charakterisierung von $\mathscr{Z}(K)$

Wir schaffen nun den Übergang in die Algebra, indem wir zeigen, dass die Menge der konstruierbaren Punkte einen Körper bildet.

Satz 3.3.1. *Die Menge $\mathscr{Z}(K)$ aller aus $K \subseteq \mathbb{C}$ mit Zirkel und Lineal konstruierbaren Zahlen bildet einen Teilkörper von $\mathbb{C}$.*

Beweis. Da $0, 1 \in \mathscr{Z}(K)$ gilt, müssen wir nur noch zeigen, dass für alle $a, b \in \mathscr{Z}(K)$ mit $a \neq 0$ auch $a + b, a \cdot b, -a, a^{-1} \in \mathscr{Z}(K)$ gilt.

- $-a$: Wir erhalten $-a$ durch Spiegeln von a an 0, ganz analog zu Abbildung (3.2, vi)).
- a^{-1}: Wir können zu gegebenem $a = r \cdot e^{i\varphi}$ auch $\overline{a} = r \cdot e^{-i\varphi}$ konstruieren (indem man beispielsweise die zur Geraden durch $0, 1$ senkrechte Gerade durch a konstruiert, ebenso den Kreis um 0 durch a; die beiden Schnittpunkte dieser Geraden mit dem Kreis sind $a, \overline{a}$). In Schritt 1 der Abbildung (3.3) können wir nach Beispiel (3.2.1,iii)) die zur Verbindungsgeraden durch i und r parallele Gerade durch 1 konstruieren. Aus dem Strahlensatz folgt, dass der Schnittpunkt dieser Geraden mit der y-Achse $i \cdot r^{-1}$ ist. In Schritt 2 konstruieren wir die Gerade durch 0 und $\overline{a}$ sowie den Kreis um 0 durch $i \cdot r^{-1}$. Die Schnittpunkte dieser Geraden mit dem Kreis sind gerade $\pm a^{-1} = \pm \frac{1}{r} \cdot e^{-i\varphi}$.

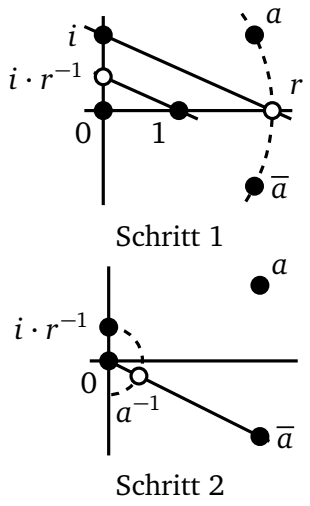
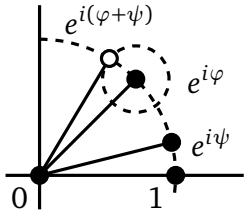


Abbildung 3.3: Konstruktion von a^{-1}

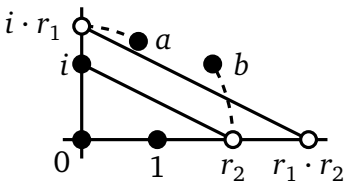
- $a + b$: Nach Beispiel (3.2.1,i)) können wir den Mittelpunkt $\frac{a+b}{2}$ konstruieren. Entweder ist $a+b=0$, dann ist $a+b$ per Definition konstruierbar, ansonsten erhalten wir $a + b$ aus der Spiegelung von 0 an $\frac{a+b}{2}$ wie in Abbildung (3.2, vi)).
- $a \cdot b$: Wir können annehmen, dass $b \neq 0$ gilt, denn sonst ist die Aussage klar. Wir schreiben a, b als $a = r_1 \cdot e^{i\varphi}$, $b = r_2 \cdot e^{i\psi}$. Wir können dann jeweils $e^{i\varphi}$ und $e^{i\psi}$ als Schnittpunkt der Geraden durch 0 und a bzw. b und dem Einheitskreis konstruieren. In Schritt 1 der Abbildung (3.4) konstruieren wir aus diesen beiden Punkten $e^{i(\varphi+\psi)}$, indem wir einen Kreis um $e^{i\varphi}$ mit Radius $r = |e^{i\psi} - 1|$ bilden, falls $r \neq 0$ (der Fall $e^{i\psi} = 1$ ist trivial). Da $e^{i(\varphi+\psi)}$ auf dem Einheitskreis liegt und die Gleichung $|e^{i(\varphi+\psi)} - e^{i\varphi}| = |e^{i\psi} - 1|$ erfüllt, ist $e^{i(\varphi+\psi)}$ einer der beiden so konstruierten Schnittpunkte.

  In Schritt 2 konstruieren wir $r_1 \cdot r_2$. Dazu konstruieren wir ir_1 und r_2 als Schnittpunkte der y-Achse bzw. x-Achse mit den Kreisen um 0 durch b bzw. a. Wir können nach Beispiel (3.2.1,iii)) die Gerade durch ir_1 konstruieren, die parallel zur Geraden durch i und r_2 verläuft. Diese schneidet nach dem Strahlensatz die x-Achse in $r_1 \cdot r_2$.

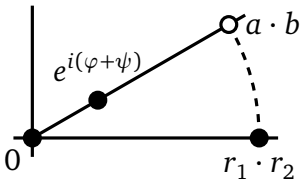
  Abschließend konstruieren wir $a \cdot b$ in Schritt 3 als Schnittpunkt der Geraden durch $0, e^{i(\varphi+\psi)}$ mit dem Kreis um 0 durch $r_1 \cdot r_2$ (der zweite Schnittpunkt ist $-a \cdot b$).



Schritt 1



Schritt 2



Schritt 3

Abbildung 3.4: Konstruktion von $a \cdot b$

□

Korollar 3.3.2. *Es gilt:*

i) $\mathbb{Q}[i] = \{a + ib \in \mathbb{C} | a, b \in \mathbb{Q}\} \subseteq \mathscr{Z}(K)$

ii) $z \in \mathscr{Z}(K) \Leftrightarrow \mathrm{Re}(z), \mathrm{Im}(z) \in \mathscr{Z}(K)$

iii) $z \in \mathscr{Z}(K) \Rightarrow \pm\sqrt{z} \in \mathscr{Z}(K)$

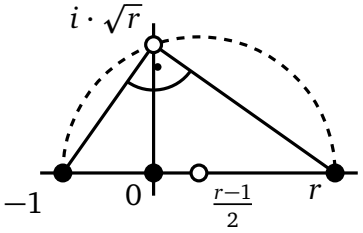


Abbildung 3.5: Konstruktion von $\sqrt{z}$

Beweis.

i) Wir haben schon gesehen, dass $\mathbb{Z} \subseteq \mathscr{Z}(K)$ gilt. Da nach Satz (3.3.1) $\mathscr{Z}(K)$ ein Körper ist, folgt aus $i \in \mathscr{Z}(K)$ die Aussage $\mathbb{Q}[i] \subseteq \mathscr{Z}(K)$.

ii) "⇒" Da aus $z \in \mathscr{Z}(K)$ auch $\overline{z} \in \mathscr{Z}(K)$ folgt, sind nach Beispiel (3.2.1,i)) auch $\mathrm{Re}(z) = \frac{z+\overline{z}}{2}$ und $\mathrm{Im}(z) = \frac{z-\overline{z}}{2i}$ konstruierbar.

"⇐" Da $i \in \mathscr{Z}(K)$ und $\mathscr{Z}(K)$ ein Köper ist, folgt $\mathrm{Re}(z) + i \cdot \mathrm{Im}(z) \in \mathscr{Z}(K)$.

iii) Sei $z = r \cdot e^{i\cdot\varphi} \in \mathscr{Z}(K)$. Wie wir schon gesehen haben, können wir $r = |z|$ und $e^{i\cdot\varphi}$ konstruieren (siehe Abbildung (3.4)). Weiter können wir den Mittelpunkt $\frac{r-1}{2}$ und den Umkreis durch r konstruieren. Der Schnittpunkt mit der y-Achse ist $i \cdot \sqrt{r}$, denn nach dem Satz des Thales ist das in Abbildung (3.5) eingezeichnete Dreieck rechtwinklig und die Aussage folgt aus dem Höhensatz.

Weiter können wir nach Beispiel (3.2.1,iv)) Winkel halbieren, d.h. wir können auch $e^{i\cdot\varphi/2}$ konstruieren. Da $\mathscr{Z}(K)$ ein Körper ist, gilt damit $\pm\sqrt{z} = \pm\sqrt{r}\cdot e^{i\cdot\varphi/2} \in \mathscr{Z}(K)$.

□

Lemma 3.3.3. *Der Körper $\mathscr{Z}(K)$ aller aus $K \subseteq \mathbb{C}$ mit Zirkel und Lineal konstruierbaren Elemente ist der Durchschnitt aller Teilkörper L von $\mathbb{C}$ mit den folgenden Eigenschaften:*

(1) $K \subseteq L$

(2) $z \in L \Rightarrow \overline{z} \in L$

(3) $z \in L \Rightarrow \pm\sqrt{z} \in L$

Beweis. Sei $M := \{L \subseteq \mathbb{C} | L$ ist ein Teilkörper von $\mathbb{C}$, der (1)-(3) erfüllt$\}$ die Menge aller Teilkörper von $\mathbb{C}$ mit den Eigenschaften *(1)* bis *(3)*. Wir wollen die Gleichheit

$$\mathscr{Z}(K) = \bigcap_{L\in M} L =: \tilde{L}$$

zeigen, dazu zeigen wir beide Inklusionen.
Wir haben schon gesehen, dass $\mathscr{Z}(K)$ alle drei Eigenschaften erfüllt, somit gilt $\mathscr{Z}(K) \in M$ und damit $\mathscr{Z}(K) \supseteq \tilde{L}$. Für die andere Inklusion halten wir zunächst fest, dass sich die Eigenschaften *(1)* bis *(3)* auf $\tilde{L}$ übertragen. Mit Eigenschaft *(3)* folgt $i = \sqrt{-1} \in \tilde{L}$, aus *(2)* folgt dann für alle $z \in \mathbb{C}$:

$$z \in \tilde{L} \Leftrightarrow \mathrm{Re}(z), \mathrm{Im}(z) \in \tilde{L}$$

Um die andere Inklusion zu zeigen, bietet sich aufgrund der Definition von $\mathscr{Z}(K)$ vollständige Induktion an, d.h. wir zeigen $K_n \subseteq \tilde{L}$ für alle $n \in \mathbb{N}_0$. Für $n = 0$ gilt $K_0 = K \subseteq \tilde{L}$ nach Voraussetzung, daher nehmen wir nun $K_n \subseteq \tilde{L}$ für ein $n \in \mathbb{N}_0$ an. Mit $K_{n+1} = K_n \cup S_{g,g}(K_n) \cup S_{g,k}(K_n) \cup S_{k,k}(K_n)$ gilt es nun zu zeigen, dass $S_{g,g}(K_n), S_{g,k}(K_n), S_{k,k}(K_n) \subseteq \tilde{L}$ gilt.

- $S_{g,g}(K_n)$: Seien $a_1, b_1, a_2, b_2 \in K_n \subseteq \tilde{L}$ mit $a_1 \neq b_1$ und $a_2 \neq b_2$, so dass die Gerade durch a_1 und b_1 nicht parallel zur Geraden durch a_2 und b_2 ist. Der Schnittpunkt z der beiden Geraden erfüllt die Gleichungen

  $$z = a_1 + t(b_1 - a_1)$$
  $$z = a_2 + s(b_2 - a_2)$$

  für ein $s, t \in \mathbb{R}$. Durch Subtrahieren erhält man die beiden Gleichungen

  $$0 = \mathrm{Re}(a_2 - a_1) + s\cdot\mathrm{Re}(b_2 - a_2) - t\cdot\mathrm{Re}(b_1 - a_1)$$
  $$0 = \mathrm{Im}(a_2 - a_1) + s\cdot\mathrm{Im}(b_2 - a_2) - t\cdot\mathrm{Im}(b_1 - a_1)$$

  Dieses lineare Gleichungssystem mit Koeffizienten in $\tilde{L}$ besitzt nach Voraussetzung eine eindeutige Lösung in $\mathbb{C}$ (da die Geraden nicht parallel sind), für die Lösungen in s und t gilt damit zusätzlich $s, t \in \tilde{L}$ nach der Cramerschen Regel. Daher gilt auch $z = a_1 + t(b_1 - a_1) \in \tilde{L}$ und somit folgt $S_{g,g}(K_n) \subseteq \tilde{L}$.

- $S_{g,k}(K_n)$: Seien nun $a, b, m, c \in K_n \subseteq \tilde{L}$ mit $a \neq b$ und $m \neq c$. Ein möglicher Schnittpunkt $z \in \mathbb{C}$ der Geraden durch a und b mit dem Kreis um m durch c erfüllt die beiden Gleichungen

  $$z = a + t(b - a) \tag{1}$$
  $$|z - m|^2 = |m - c|^2 \tag{2}$$

für ein $t \in \mathbb{R}$. Durch Einsetzen von Gleichung (1) in (2) und Ausmultiplizieren erhält man eine Gleichung der folgenden Gestalt für t:

$$k_1 \cdot t^2 + k_2 \cdot t + k_3 = 0 \tag{3}$$

mit Koeffizienten $k_1, k_2, k_3 \in \tilde{L} \cap \mathbb{R}$ und $k_1 \neq 0$. Falls $\left(\frac{k_2}{2k_1}\right)^2 - \frac{k_3}{k_1} \geq 0$, so besitzt die Gleichung (3) nach der pq-Formel reelle Lösungen in t der Form

$$t = -\frac{k_2}{2k_1} \pm \sqrt{\left(\frac{k_2}{2k_1}\right)^2 - \frac{k_3}{k_1}}$$

(andernfalls gibt es keine reelle Lösung für t und es gibt somit überhaupt keinen Schnittpunkt). Nach Eigenschaft *(3)* gilt sogar $t \in \tilde{L} \cap \mathbb{R}$ und damit wieder $z = a + t \cdot (b - a) \in \tilde{L}$. Dies beweist $S_{g,k}(K_n) \subseteq \tilde{L}$.

- $S_{k,k}(K_n)$: Wieder seien $a, b, x, y \in K_n \subseteq \tilde{L}$ mit $a \neq b$, $a \neq x$ und $x \neq y$. Wir definieren $r_1 := |a-b|$, $r_2 := |x - y|$ und $d := |a - x|$. Die möglichen Schnittpunkte der beiden Kreise um a und x durch b und y liegen auf der Geraden

$$g = \left\{ z \in \mathbb{C} \,\middle|\, z = m + t \cdot i(x - a), t \in \mathbb{R} \right\}$$

für ein $m \in \mathbb{C}$ (Multiplikation mit i entspricht einer Drehung um 90°). Wir wollen nun $m \in \tilde{L}$ zeigen, dazu erhalten wir folgende Gleichungen aus Abbildung (3.6):

$$r_1^2 = d_1^2 + h^2 \tag{4}$$
$$r_2^2 = d_2^2 + h^2 \tag{5}$$
$$d_2 = d - d_1 \tag{6}$$

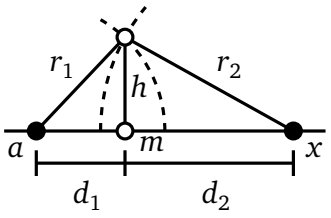


Abbildung 3.6: Schnittpunkte zweier Kreise

Durch Subtrahieren von Gleichung (5) und (4) sowie anschließendes Einsetzen von Gleichung (6) erhalten wir

$$d_1 = \frac{r_1^2 - r_2^2 + d^2}{2 \cdot d} \in \tilde{L} \cap \mathbb{R}$$

und damit

$$m = a + \frac{d_1}{d} \cdot (x - a) \in \tilde{L}.$$

Daher sind die Schnittpunkte der beiden Kreise die Schnittpunkte eines Kreises mit der Geraden g, womit wir ganz analog zum Fall $S_{g,k}(K_n)$ die Bedingung $z \in \tilde{L}$ für einen möglichen Schnittpunkt z erhalten, und somit auch $S_{k,k}(K_n) \subseteq \tilde{L}$.

Zusammengefasst haben wir damit $K_{n+1} = K_n \cup S_{g,g}(K_n) \cup S_{g,k}(K_n) \cup S_{k,k}(K_n) \subseteq \tilde{L}$ bewiesen, nach Induktion folgt somit $\mathscr{Z}(K) = \bigcup_{n \in \mathbb{N}_0} K_n \subseteq \tilde{L}$. Damit sind beide Inklusionen gezeigt und es gilt Gleichheit. □

Im nächsten Theorem geht es nun darum, ein Kriterium anzugeben, ob ein gegebenes $z \in \mathbb{C}$ konstruierbar ist oder nicht.

Theorem 3.3.4 (Version 1). *Folgende Aussagen sind für $z \in \mathbb{C}$ äquivalent:*

i) $z \in \mathscr{Z}(K)$

ii) Es existiert eine aufsteigende Kette von Körpererweiterungen $\mathbb{Q}(K \cup \overline{K}) = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_n \subseteq \mathbb{C}$ mit $z \in L_n$ und $[L_j : L_{j-1}] = 2$ für alle $j = 1, ..., n$ (wobei $\overline{K} = \{\overline{k} \in \mathbb{C} | k \in K\}$).

Die folgende Beweisidee stammt aus [KM13, 22.1.4].

Beweis.

- " *i)* $\Leftarrow$ *ii)* ": Sei eine Körperkette wie in *ii)* gegeben. Nach Korollar (3.3.2) und Lemma (3.3.3) gilt $L_0 = \mathbb{Q}(K \cup \overline{K}) \subseteq \mathscr{Z}(K)$. Da $[L_1 : L_0] = 2$ gilt, gibt es zu einem gegebenen $z \in L_1 \backslash L_0$ Koeffizienten $a, b \in L_0$ mit $z^2 + a \cdot z + b = 0$, da die Elemente $1, z, z^2$ linear abhängig über L_0 sein müssen. Definiert man $c := z + \frac{a}{2}$, so gilt $c^2 = z^2 + a \cdot z + \frac{a^2}{4} = -b + \frac{a^2}{4} \in L_0$ und $L_1 = L_0(c)$ wegen $c \notin L_0$. Da in $\mathscr{Z}(K)$ auch Quadratwurzeln von konstruierbaren Elementen enthalten sind, folgt aus $c^2 \in L_0 \subseteq \mathscr{Z}(K)$ auch $c \in \mathscr{Z}(K)$ und somit $L_1 = L_0(c) \subseteq \mathscr{Z}(K)$. Induktiv erhält man letztendlich auch $L_n \subseteq \mathscr{Z}(K)$ und damit $z \in L_n \subseteq \mathscr{Z}(K)$.

- " *i)* $\Rightarrow$ *ii)* ": Sei nun $M \subseteq \mathbb{C}$ die Menge aller Elemente, für die solch eine Körperkette existiert. Wir zeigen nun, dass M ein Körper ist, welcher die Eigenschaften *(1),(2)* und *(3)* aus Lemma (3.3.3) erfüllt. Daraus folgt $\mathscr{Z}(K) \subseteq M$ und somit existiert solch eine geforderte Körperkette für $z \in \mathscr{Z}(K)$. Die Menge M enthält $0, 1$ und ist folglich nicht leer. Seien nun $a, b \in M$, dann gibt es $a_1, ...a_n \in M$ und $b_1, ...b_m \in M$ mit

$$a \in L_0(a_1, ..., a_n) \supseteq L_0(a_1, ..., a_{n-1}) \supseteq \cdots \supseteq L_0(a_1) \supseteq L_0$$
$$b \in L_0(b_1, ..., b_m) \supseteq L_0(b_1, ..., b_{m-1}) \supseteq \cdots \supseteq L_0(b_1) \supseteq L_0$$

  und $a_{i+1}^2 \in L_0(a_1, ..., a_i)$ sowie $b_{j+1}^2 \in L_0(b_1, ..., b_j)$ für alle $i = 0, ..., n-1$ und $j = 0, ..., m-1$, wie wir schon in der anderen Implikation gesehen haben. Für die Körperkette

$$M_{a,b} := L_0(a_1, ..., a_n, b_1, ..., b_m) \supseteq \cdots \supseteq L_0(a_1, ..., a_n, b_1) \supseteq L_0(a_1, ..., a_n) \supseteq \cdots \supseteq L_0(a_1) \supseteq L_0$$

  gilt $[F : E] \leq 2$ für zwei aufeinanderfolgende Körper $E \subseteq F$ in der Körperkette und $a, b \in M_{a,b}$. Somit gilt $a + b, a \cdot b, a^{-1}, -a \in M_{a,b} \subseteq M$ und M ist daher ein Körper.

  Es bleibt zu zeigen, dass M die drei Eigenschaften aus Lemma (3.3.3) erfüllt. *(1)* folgt direkt aus $K \subseteq L_0 \subseteq M$. Sei $z \in M$, d.h. es gibt eine Körperkette $\mathbb{Q}(K \cup \overline{K}) = L_0 \subseteq \cdots \subseteq L_n$ mit $z \in L_n$ und $[L_j : L_{j-1}] = 2$ für alle $j = 1, ..., n$. Wegen $[L_n(\sqrt{z}) : L_n] \leq 2$ gilt somit auch $\sqrt{z} \in M$ und Eigenschaft *(3)* ist erfüllt. Sei nun $a \in M$, dann existiert wieder nach Definition von M eine Körperkette $L_0 \subseteq \cdots \subseteq L_n$ mit den Eigenschaften aus *ii)*. Wegen $\overline{\mathbb{Q}} = \mathbb{Q}$ und $\overline{K \cup \overline{K}} = K \cup \overline{K}$ gilt $\overline{L_0} = L_0$, da jedes Element aus L_0 durch eine endliche Verknüpfung von Elementen aus $\mathbb{Q}$ und $K \cup \overline{K}$ darstellbar ist. Weiter ist $\overline{L_j}$ ein Körper für alle $j = 0, ..., n$, wie man leicht einsieht. Es gilt damit

$$\overline{L_{j+1}} = \overline{L_j(a_j)} = \overline{L_j + a_j \cdot L_j} = \overline{L_j} + \overline{a_j} \cdot \overline{L_j} = \overline{L_j}(\overline{a_j})$$

  für ein $a_j \in L_{j+1}$ mit $a_j^2 \in L_j$ und damit auch $\overline{a_j}^2 = \overline{a_j^2} \in \overline{L_j}$, und somit $[\overline{L_{j+1}} : \overline{L_j}] \leq 2$. Dies zeigt $\overline{a} \in M$, da $L_0 = \overline{L_0} \subseteq \cdots \subseteq \overline{L_n}$ eine Körperkette mit den gewünschten Eigenschaften ist. Damit erfüllt M auch Eigenschaft *(2)* und somit gilt $\mathscr{Z}(K) \subseteq M$, was zu zeigen war.

□

Das obige Theorem impliziert direkt folgendes Korollar:

Korollar 3.3.5. *Gilt $z \in \mathscr{Z}(K)$, so folgt $[Q_0(z) : Q_0] = 2^r$ für ein $r \in \mathbb{N}_0$ und $Q_0 := \mathbb{Q}(K \cup \overline{K})$.*

Beweis. Sei $z \in \mathscr{Z}(K)$, dann existiert nach Theorem (3.3.4) eine Körperkette $\mathbb{Q}(K \cup \overline{K}) = L_0 \subseteq \cdots \subseteq L_n$ mit $[L_{j+1} : L_j] = 2$ und $z \in L_n$. Daraus folgt $[L_n : L_0] = 2^n$ und somit $[L_n : L_0(z)] \cdot [L_0(z) : L_0] = 2^n \Rightarrow [L_0(z) : L_0] = 2^r$ für ein $r \in \mathbb{N}_0$. □

Wir werden nun eine zweite Fassung dieses Theorems aufstellen und beweisen, welche Mittel der Galoistheorie benötigt. Das Theorem und der Beweis richten sich nach [Bos09, 6.4, Satz 1].

Theorem 3.3.6 (Version 2)**.** *Folgende Aussagen sind für $z \in \mathbb{C}$ äquivalent:*

i) $z \in \mathscr{Z}(K)$

ii) Es gibt eine Galoiserweiterung $L/\mathbb{Q}(K \cup \overline{K})$ mit $z \in L$ und $[L : \mathbb{Q}(K \cup \overline{K})] = 2^n$ für ein $n \in \mathbb{N}_0$.

Beweis.

- " *i) $\Rightarrow$ ii)* ": Sei $z \in \mathscr{Z}(K)$, dann existiert nach Theorem (3.3.4) eine Körperkette $\mathbb{Q}(K \cup \overline{K}) = L_0 \subseteq L_1 = L_0(a_1) \subseteq \cdots \subseteq L_n = L_{n-1}(a_n)$ mit $z \in L_n$ und $a_{j+1}^2 \in L_j$ für alle $j = 0, ..., n-1$. Nach Satz (2.3.8) existiert eine algebraische Körpererweiterung M_n/L_n, sodass M_n/L_0 normal ist. Wir zeigen zuerst, dass $G_n := \{\sigma : L_n \to M_n | \sigma \text{ ist } L_0\text{- Homomorphismus}\}$ endlich ist. Dies zeigen wir wie folgt durch Induktion: Sei $\sigma \in G_n$. Wegen $L_n = L_0(a_1, ..., a_n)$ und $a_1^2 - c_1 = 0$ für ein $c_1 \in L_0$ gilt

  $$0 = \sigma(0) = \sigma(a_1^2 - c_1) = \sigma(a_1)^2 - c_1 \Rightarrow \sigma(a_1) = \pm a_1.$$

  Somit gibt es nur 2 mögliche Bilder für a_1 unter $\sigma \in G_n$. Wir nehmen nun an, dass es für jedes a_j mit $j < n$ nur endlich viele mögliche Bilder unter $\sigma \in G_n$ gibt. Da die Bilder von Elementen aus $L_0(a_1, ..., a_{n-1})$ unter $\sigma \in G_n$ eindeutig bestimmt durch die Bilder von $a_1, ..., a_{n-1}$ sind, gibt es auch für jedes Element aus $L_0(a_1, ..., a_{n-1})$ nur endlich viele mögliche Bilder unter $\sigma \in G_n$. Mit $0 = \sigma(a_n^2 - c_n) = \sigma(a_n)^2 - \sigma(c_n) \Rightarrow \sigma(a_n) = \pm\sqrt{\sigma(c_n)}$ folgt damit, dass es auch für a_n nur endlich viele mögliche Bilder unter $\sigma \in G_n$ gibt. Daher kann es nur endlich viele L_0-Homomorphismen $\sigma : L_n \to M_n$ geben, d.h. G_n ist endlich.

  Wir zeigen nun die Implikation, indem wir L als die normale Hülle L_n' wie in Satz (2.3.8) wählen. Sei also $|G_n| = r$ und

  $$L_n' = L_0(\{\sigma_i(L_n) | \sigma_i \in G_n\}) = L_0(\{\sigma_i(a_j) | i = 1, ..., r,\ j = 1, ..., n\}).$$

  Es gilt $\sigma_i(a_j)^2 = \sigma_i(a_j^2) \in \sigma_i(L_{j-1}) = L_0(\sigma_i(a_1), ..., \sigma_i(a_{j-1}))$ für $j = 2, ..., n$ und $\sigma_i(a_1)^2 \in L_0$. Mit $\tilde{L} := L_0(\sigma_1(a_1), ...\sigma_1(a_n), \sigma_2(a_1), ..., \sigma_r(a_1), ..., \sigma_r(a_{n-1}))$ folgt dann für den Körperindex

  $$[L_n' : L_0] = \underbrace{[L_n' : \tilde{L}]}_{\in\{1,2\}} \cdots \underbrace{[L_0(\sigma_1(a_1), \sigma_1(a_2)) : L_0(\sigma_1(a_1))]}_{\in\{1,2\}} \cdot \underbrace{[L_0(\sigma_1(a_1)) : L_0]}_{\in\{1,2\}}$$

  und somit ist $[L_n' : \mathbb{Q}(K \cup \overline{K})] = 2^k$ für ein $k \in \mathbb{N}_0$. Als endliche und damit algebraische Erweiterung über einem Körper der Charakteristik 0 ist die Körpererweiterung $L_n'/\mathbb{Q}(K \cup \overline{K})$ nach Satz (2.3.2) separabel. Nach Konstruktion von L_n' ist sie auch normal und damit eine Galoiserweiterung mit der gewünschten Eigenschaft.

- " *i) $\Leftarrow$ ii)* ": Sei $L/\mathbb{Q}(K \cup \overline{K})$ eine Galoiserweiterung mit $z \in L$ und $[L : \mathbb{Q}(K \cup \overline{K})] = 2^k$ für ein $k \in \mathbb{N}_0$. Wieder können wir Theorem (3.3.4) ausnutzen, indem wir zeigen, dass eine Körperkette $\mathbb{Q}(K \cup \overline{K}) = L_0 \subseteq \cdots \subseteq L_n$ mit $z \in L_n$ und $[L_{j+1} : L_j] = 2$ für alle $j = 0, ..., n-1$ existiert. Wegen $|\mathrm{Gal}(L/L_0)| = [L : L_0] = 2^k$ mit $L_0 := \mathbb{Q}(K \cup \overline{K})$ ist $\mathrm{Gal}(L/L_0)$ eine 2-Gruppe und damit auflösbar nach Satz (2.2.1), d.h. es gibt eine aufsteigende Kette von Untergruppen

  $$\{\mathrm{id}\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_k = \mathrm{Gal}(L/L_0)$$

  mit $[G_{j+1} : G_j] = 2$ für alle $j = 0, ..., k-1$.

Aus der Galoistheorie folgt nun, dass

$$L_0 = L^{G_k} \subseteq L^{G_{k-1}} \subseteq \cdots \subseteq L^{G_0} = L$$

eine aufsteigende Körperkette ist mit

$$[L^{G_j} : L^{G_{j+1}}] = \frac{[L^{G_j} : L_0]}{[L^{G_{j+1}} : L_0]} = \frac{[G_k : G_j]}{[G_k : G_{j+1}]} = \frac{[G_k : G_{j+1}] \cdot [G_{j+1} : G_j]}{[G_k : G_{j+1}]} = [G_{j+1} : G_j] = 2$$

nach Satz (2.3.9). Somit haben wir die gesuchte Körperkette gefunden.

□

3.4 Lösbarkeit der antiken Probleme mit Zirkel und Lineal

Wir wollen nun klären, welche der antiken Probleme (2.4.1) mit Zirkel und Lineal lösbar sind.

Satz 3.4.1. *Die drei antiken Probleme sind nicht mit Zirkel und Lineal lösbar.*

Beweis.

- Zum delischen Problem: Das Polynom X^3-2 ist nach dem Eisensteinschen Irreduzibilitätskriterium (2.3.6) irreduzibel in $\mathbb{Q}[X]$ und daher das Minimalpolynom von $\sqrt[3]{2}$ über $\mathbb{Q}$. Nach Satz (2.3.7) gilt somit $[\mathbb{Q}(a) : \mathbb{Q}] = \operatorname{grad}(X^3 - 2) = 3$. Aus Korollar (3.3.5) folgt daher $a \notin \mathscr{Z}(\{0,1\})$.
- Zur Winkeldreiteilung: Sei $\xi_3 := e^{2\pi i/3}$ und $\xi_9 := e^{2\pi i/9}$, dann folgt aus Satz (2.3.10):

  $$[\mathbb{Q}(\xi_9) : \mathbb{Q}(\xi_3)] = \frac{[\mathbb{Q}(\xi_9) : \mathbb{Q}]}{[\mathbb{Q}(\xi_3) : \mathbb{Q}]} = \frac{\varphi(9)}{\varphi(3)} = \frac{6}{2} = 3$$

  Wieder folgt somit $\xi_9 \notin \mathscr{Z}(\{0,1,\xi_3\})$, da der Grad von ξ_9 über $\mathbb{Q}(\xi_3)$ keine Zweierpotenz ist.
- Zur Quadratur des Kreises: Wäre $\sqrt{\pi} \in \mathscr{Z}(\{0,1\})$, dann auch $\pi \in \mathscr{Z}(\{0,1\})$. Da π transzendent über $\mathbb{Q}$ ist, folgt $[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$, was ebenfalls keine Zweierpotenz ist und damit abermals $\pi \notin \mathscr{Z}(\{0,1\})$.

□

4 Konstruierbarkeit mit Origami

4.1 Überblick

In diesem Kapitel wollen wir analog zum vorigen Kapitel vorgehen und Konstruierbarkeit mit Origami studieren. Unser Leitfaden wird dabei [Fuc11] sein, viele Resultate lassen sich jedoch aus der Konstruierbarkeit mit Zirkel und Lineal auf Origami übertragen, da Konstruktionen mit Origami dahingehend mächtiger sind, dass mit Zirkel und Lineal konstruierbare Punkte ebenso mit Origami konstruierbar sind. Unsere Zeichenebene wählen wir wie üblich als $\mathbb{C}$. In den folgenden Abbildungen in diesem Kapitel stellen wir die neu konstruierten Geraden gestrichelt, die schon gegebenen durchgezogen dar.

4.2 Konstruktionen mit Origami

Definition (nach [Lan])**.** *Sei $K \subseteq \mathbb{C}$ mit $0, 1 \in K$ gegeben. Die Menge $K_n \subseteq \mathbb{C}$ der in $n \in \mathbb{N}_0$ Schritten aus K mit Origami konstruierbaren Zahlen **und** Geraden ist folgendermaßen rekursiv definiert:*

$$K_n := \begin{cases} K, & \text{falls } n = 0 \\ K_{n-1} \cup S(K_{n-1}) \cup G(K_{n-1}), & \text{sonst} \end{cases}$$

Dabei bezeichnet $S(K_{n-1})$ die Menge aller Schnittpunkte zweier nicht paralleler Geraden aus K_{n-1} und $G(K_{n-1})$ die Menge aller auf folgende Weisen aus K_{n-1} konstruierten Geraden:
Seien die Punkte $p_1, p_2 \in K_{n-1}$ mit $p_1 \neq p_2$ und, falls existent, die Geraden $l_1, l_2 \in K_{n-1}$ mit $l_1 \neq l_2$ gegeben.

(O1) *Die Gerade durch p_1 und p_2 ist konstruierbar.*

(O2) *Die Mittelsenkrechte zur Verbindungsgeraden von p_1 und p_2 ist konstruierbar.*

(O3) *Die Gerade h ist konstruierbar, sodass die Spiegelung von l_1 an h gerade l_2 entspricht.*

(O4) *Die Gerade durch p_1 senkrecht zu l_1 ist konstruierbar.*

(O5) *Die Gerade h durch p_2 ist konstruierbar, so dass die Spiegelung von p_1 an h auf l_1 liegt.*

(O6) *Es ist eine Gerade h konstruierbar, so dass die Spiegelung von p_1 bzw. p_2 an h auf l_1 bzw. l_2 liegt, falls $p_1 \notin l_1$ und $p_2 \notin l_2$.*

(O7) *Sind l_1 und l_2 nicht parallel, so ist eine zu l_2 senkrechte Gerade h konstruierbar, so dass die Spiegelung von p_1 an h auf l_1 liegt.*

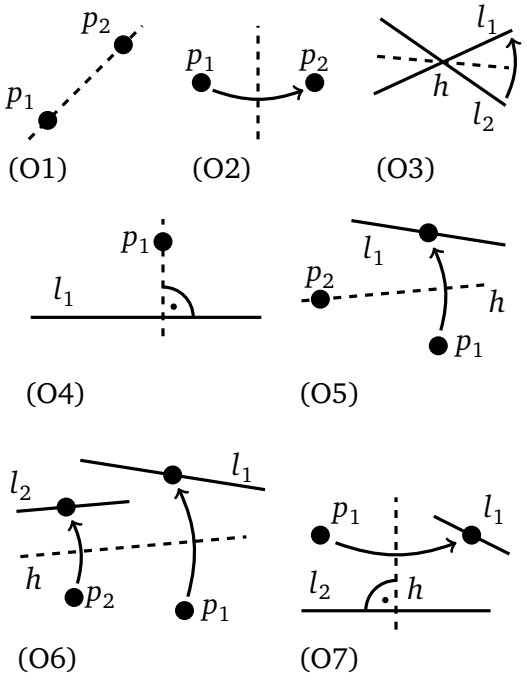


Abbildung 4.1: Konstruktionen mit Origami

Die Menge $\mathcal{O}(K) \subseteq \mathbb{C}$ aller aus K mit Origami konstruierbaren Zahlen ist definiert als

$$\mathcal{O}(K) := \left(\bigcup_{n=0}^{\infty} K_n \right) \cap \mathbb{C}.$$

Bemerkung 4.2.1. *Die Axiome (O5) und (O6) sind dahingehend unpräzise, dass die geforderte Gerade h gar nicht existieren muss. Auch muss die Gerade h in (O3), (O5) und (O6) nicht eindeutig sein. Wir wollen die Axiome daher so verstehen: Falls eine Gerade h die gewünschten Eigenschaften erfüllt, so ist sie auch konstruierbar, d.h. wir nehmen sie in die Menge $G(K_{n-1})$ mit auf. Mit folgender Definition für den Abstand eines Punktes $p \in \mathbb{C}$ von einer Geraden $g \subseteq \mathbb{C}$*

$$d(p, g) := \inf_{z \in g} |z - p|$$

ergibt sich damit beispielsweise als notwendige und hinreichende Bedingung für die Existenz von h in (O5):

$$|p_1 - p_2| \geq d(p_2, l_1)$$

Sind nämlich $p_1, p_2 \in \mathbb{C}$ und $l_1 \subseteq \mathbb{C}$ wie in der Definition gegeben, so gilt für den an h gespiegelten Punkt p_1' sicherlich $|p_2 - p_1| = |p_2 - p_1'|$ und p_1' liegt somit auf dem Kreis um p_2 durch p_1. Die erforderliche Bedingung ergibt sich daraus direkt, da wir mit (O5) nach dieser Überlegung Schnitte von Kreisen und Geraden suchen. Äquivalente Bedingungen zur Existenz von h in (O6) zu finden stellt sich als bedeutend schwieriger heraus. Wir geben daher nur eine kurze Erläuterung ohne Beweis an, siehe dazu [Lan, Axiom 6 and Cubic Curves].

Hat man eine Gerade l_1 (o.B.d.A. ist l_1 die x-Achse) und zwei Punkte $p_1, p_2 \in \mathbb{C}$ gegeben, so kann man p_1 sicherlich auf jeden Punkt $l_1(t) = t \in \mathbb{R}$ der Gerade l_1 falten. Spiegelt man nun p_2 an dieser dadurch entstandenen Faltgerade und nennt den gespiegelten Punkt $p_2'(t)$, so erhält man eine stetige (kubische) Kurve $\gamma : t \mapsto p_2'(t)$, mit $Re(p_2'(t)) \to \pm\infty$ für $t \to \pm\infty$ und $Im(p_2'(t))$ ist beschränkt über alle $t \in \mathbb{R}$ (Abbildung (4.2)). Die Gerade h aus (O6) existiert also genau dann, wenn die Gerade l_2 die Kurve γ in mindestens einem Punkt schneidet. Sind l_1 und l_2 nicht parallel, so folgt aus der Stetigkeit von γ und obiger Eigenschaft auch schon, dass es immer mindestens einen Schnittpunkt und somit auch eine Gerade h mit den Eigenschaften aus (O6) gibt.

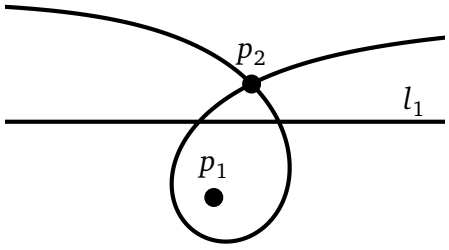


Abbildung 4.2: Kurve aller möglichen Spiegelungen von p_2

Die Axiome *(O3)* bis *(O7)* machen den doch eher technisch erscheinenden Trick notwendig, die Geraden ebenfalls zu K_n hinzuzufügen, da wir auf diese Art und Weise die schon konstruierten Punkte und Geraden simultan "speichern" können. In der Definition von $\mathcal{O}(K)$ müssen wir dann natürlich wieder die Geraden entfernen, was sich mit einem einfachen Schnitt realisieren lässt.
Die Axiome *(O1)* bis *(O6)* werden Humiaki Huzita zugeschrieben, *(O7)* wurde 2003 von Koshiro Hatori entdeckt, daher werden die sieben Axiome auch **Huzita–Hatori Axiome** genannt. Wie sich herausstellte, tauchten bereits alle sieben Axiome in einer Arbeit von Jacques Justin auf, sie wurden jedoch schlichtweg von vielen Mathematikern übersehen (siehe [Lan]).
Wieder werden wir ab hier voraussetzen, dass $0, 1 \in K \subseteq \mathbb{C}$ gilt. Für $z \in \mathcal{O}(K)$ werden wir wieder häufig "$z \in \mathbb{C}$ ist Origami konstruierbar" schreiben.

4.3 Eigenschaften und Charakterisierung von $\mathcal{O}(K)$

Wir wollen natürlich wieder zeigen, dass die Menge $\mathcal{O}(K)$ einen Körper bildet, dies wird fast direkt aus dem nächsten Lemma folgen.

Lemma 4.3.1. *Es gilt $\mathcal{Z}(K) \subseteq \mathcal{O}(K)$.*

Beweis. Wieder bietet sich aufgrund der Definition von $\mathcal{Z}(K)$ vollständige Induktion an, denn können wir $K_n \subseteq \mathcal{O}(K)$ (mit K_n aus der Definition von $\mathcal{Z}(K)$) für alle $n \in \mathbb{N}_0$ zeigen, so folgt damit auch schon $\mathcal{Z}(K) = \bigcup_{n\in\mathbb{N}_0} K_n \subseteq \mathcal{O}(K)$.
Für $n = 0$ gilt $K_0 = K \subseteq \mathcal{O}(K)$, unser Induktionsanfang ist damit bewiesen. Sei daher $n \in \mathbb{N}_0$ mit $K_n \subseteq \mathcal{O}(K)$ gegeben, wir müssen nun zeigen, dass $K_{n+1} \subseteq \mathcal{O}(K)$ gilt. Sei dazu $z \in K_{n+1}$, dann liegt z entweder in K oder z ist der Schnittpunkt von zwei Geraden, einem Kreis mit einer Gerade oder zweier Kreise, die aus Punkten aus K_n konstruierbar sind.

- Ist z der Schnittpunkt zweier Geraden, die durch jeweils zwei Punkte aus K_n und damit nach Induktionsvoraussetzung aus $\mathcal{O}(K)$ verlaufen, so ist z auch Origami konstruierbar, da wir die Geraden durch diese Punkte nach *(O1)* bilden können und Schnittpunkte von Geraden auch in Origami per Definition konstruierbar sind.

- Ist z der Schnittpunkt einer Geraden mit einem Kreis, wobei die Gerade durch zwei Punkte $a, b \in K_n \subseteq \mathcal{O}(K)$ (nach Induktionsvoraussetzung) verläuft und der Mittelpunkt m des Kreises sowie ein Punkt p auf dem Kreis in $K_n \subseteq \mathcal{O}(K)$ liegen, dann ist der Schnittpunkt z der Geraden mit dem Kreis wie folgt mit Origami konstruierbar:

  In Schritt 1 der Abbildung (4.3) konstruieren wir die Gerade h, welche nach *(O5)* den Punkt p auf die Gerade durch a und b spiegelt (diese existiert, da die in Bemerkung (4.2.1) angesprochene Bedingung erfüllt ist, denn nach Voraussetzung gibt es schließlich mindestens einen Schnittpunkt des Kreises mit der Geraden). Wir bezeichnen den an h gespiegelten Punkt p mit p'. Nach *(O4)* lässt sich die Gerade s senkrecht zu h durch p bilden (Schritt 2), diese verläuft ebenfalls durch p', somit ist p' der Schnittpunkt der Geraden durch a und b und der Geraden s und somit Origami konstruierbar. Der in Abbildung (4.3, Schritt 2) eingezeichnete gepunktete Kreis verdeutlicht, dass p' einer der gewünschten Schnittpunkte des Kreises mit der Geraden ist. Den möglichen zweiten Schnittpunkt des Kreises mit der Geraden erhalten wir mit der gleichen Konstruktion, indem in Schritt 1 die für h andere mögliche Gerade gewählt wird. Beide Schnittpunkte sind somit auch Origami konstruierbar.

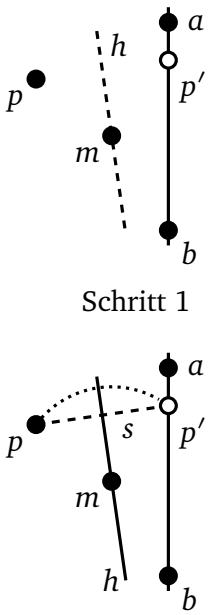


Abbildung 4.3: Schnitt von Gerade und Kreis mit Origami

- Mittels Origami lassen sich die Schnittpunkte zweier Kreise um $a, x \in K_n \subseteq \mathcal{O}(K)$ durch $b, y \in K_n \subseteq \mathcal{O}(K)$ mit $a \neq x$, $a \neq b$ und $x \neq y$ nicht auf direktem Weg bilden. Daher wollen wir dies wie im Beweis von Lemma (3.3.3) durch Zurückführen auf den Schnitt eines Kreises mit einer Geraden bewerkstelligen (siehe [Ger08, Chapter 1, 4.4]). Übernehmen wir die Bezeichnungen aus Abbildung (3.6), so reicht es zu zeigen, dass m konstruierbar ist, denn damit können wir die Gerade durch die zwei Schnittpunkte (und m) mit *(O4)* konstruieren.

  Es gilt $i \in \mathcal{O}(K)$, da nach *(O4)* die y-Achse konstruierbar ist und wir, wie schon gesehen, die Schnittpunkte $\pm i$ der y-Achse mit dem Kreis um 0 durch 1 mittels Origami konstruieren können.

Mit Origami lässt sich daher aus $a = r \cdot e^{i\varphi}, b \in \mathbb{C}$ und einer **reellen Zahl** $c \in \mathbb{R}\backslash\{0\}$ Folgendes konstruieren: $\frac{a+b}{2}$ nach *(O2)* und *(O1)* und somit auch $a+b$, $-a$, $r = |a|$, $a \cdot c$ und $\frac{a}{c}$, da wir dies mit Zirkel und Lineal ohne Schnitte zweier Kreise konstruieren können (die dazu benötigten Geraden aus Beispiel (3.2.1) lassen sich mit Origami auch ohne Schnitte zweier Kreise realisieren). Da nach dem Beweis von Lemma (3.3.3)

$$m = a + \frac{d_1}{d} \cdot (x-a) \text{ mit } d_1 = \frac{r_1^2 - r_2^2 + d^2}{2d}$$

und $r_1 = |a-b|$, $r_2 = |x-y|$, $d = |a-x|$ gilt, folgt nach obiger Überlegung somit $m \in \mathcal{O}(K)$ und damit haben wir die gewünschte Aussage gezeigt.

□

Im Beweis von Lemma(4.3.1) wurden nur die Axiome *(O1)* bis *(O5)* benutzt, somit entspricht die Menge aller nur mit *(O1)* bis *(O5)* konstruierten Punkte gerade $\mathcal{Z}(K)$, da alle Geraden und Punkte in *(O1)* bis *(O5)* auch mit Zirkel und Lineal konstruierbar sind. Auch *(O7)* ist mit Zirkel und Lineal konstruierbar, da die zu l_2 parallele Gerade durch p_1 mit Zirkel und Lineal konstruierbar ist und damit auch der Schnittpunkt dieser Geraden mit l_1. Die Mittelsenkrechte von p_1 und diesem Punkt entspricht der Geraden h aus *(O7)*. Mehr Elemente können wir also lediglich mit *(O6)* erzeugen. Die Axiome sind folglich nicht minimal gewählt, sie sind jedoch vollständig bezüglich allen Operationen, die sich durch eine einzige "Faltung" ("one-fold") beschreiben lassen, siehe [AL].

Korollar 4.3.2. *$\mathcal{O}(K)$ ist ein Körper, der folgende Eigenschaften erfüllt:*

i) $z \in \mathcal{O}(K) \Rightarrow \overline{z} \in \mathcal{O}(K)$

ii) $z \in \mathcal{O}(K) \Rightarrow \pm\sqrt{z} \in \mathcal{O}(K)$

iii) $z \in \mathcal{O}(K) \Leftrightarrow Re(z), Im(z) \in \mathcal{O}(K)$

Beweis. Mit Lemma (4.3.1) können wir direkt zeigen, dass $\mathcal{O}(K)$ ein Körper ist, der *i)*, *ii)* und *iii)* erfüllt. Seien $a, b \in \mathcal{O}(K)$ mit $a \neq 0$, dann gilt:

$$a+b, a\cdot b, -b, a^{-1}, \overline{b}, \pm\sqrt{b} \in \mathcal{Z}(K \cup \{a,b\}) \subseteq \mathcal{O}(K \cup \{a,b\}) = \mathcal{O}(K)$$

sowie wegen $i \in \mathcal{Z}(K) \subseteq \mathcal{O}(K)$

$$b \in \mathcal{O}(K) \Rightarrow \mathrm{Re}(b), \mathrm{Im}(b) \in \mathcal{Z}(K \cup \{b\}) \subseteq \mathcal{O}(K).$$

Die umgekehrte Implikation folgt schließlich aus der Körpereigenschaft und $i = \sqrt{-1} \in \mathcal{Z}(K) \subseteq \mathcal{O}(K)$, somit haben wir alle gewünschten Aussagen gezeigt. □

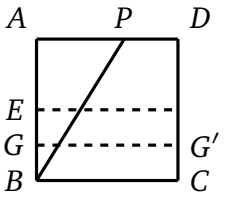
Satz 4.3.3 (Winkeldreiteilung)**.** *Mit Origami lassen sich Winkel dritteln, d.h. es gilt*

$$e^{i\varphi/3} \in \mathcal{O}(\{0, 1, e^{i\varphi}\})$$

Wir geben nun eine mögliche Konstruktion zur Drittelung eines Winkels zwischen 0 und $\pi/2$ an, anschließend beweisen wir dann die Korrektheit und begründen, warum wir daher jeden Winkel dreiteilen können.

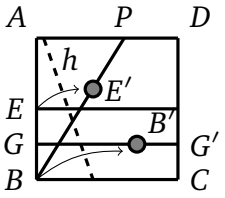
Konstruktion 4.3.4 (nach [Fuc11])**.** *Gegeben seien die Punkte $A, B, C, D \in \mathbb{C}$, o.B.d.A. können wir diese als $i, 0, 1, 1+i$ betrachten. Geraden wollen wir von nun an auch in folgender verkürzenden Schreibweise notieren: Z.B. "AB" für die Gerade durch A und B. Sei weiter $e^{i\varphi}$ mit $0 < \varphi < \pi/2$ gegeben, dann bezeichnen wir den Schnittpunkt der Gerade durch B und $e^{i\varphi}$ mit der Gerade AD mit P.*

- Schritt 1: Wir beginnen mit der Konstruktion der Mittelsenkrechte der Gerade AB nach *(O2)*, den Schnittpunkt dieser Gerade mit AB bezeichnen wir mit E. Dies wiederholen wir mit der Gerade EB und bezeichnen den neuen Schnittpunkt mit G.



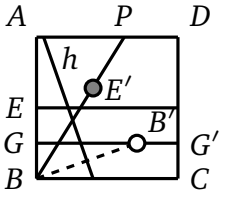
Schritt 1

- Schritt 2: Wir konstruieren die Gerade h aus *(O6)*, die E auf BP und B auf GG' spiegelt. Da die beiden an dieser Geraden gespiegelten Punkte E' und B' mit diesem Schritt noch nicht als Schnitt zweier Geraden konstruiert sind, sind diese hier grau dargestellt.



Schritt 2

- Schritt 3: Wir bilden die zur Geraden h senkrechte Gerade durch B nach *(O4)*. Diese schneidet die Gerade GG' im Punkt B', somit haben wir B' konstruiert. Der eingeschlossene Winkel zwischen B', B und C entspricht dabei $\varphi/3$. Wir erhalten $e^{i\varphi/3}$ somit als Schnitt der Geraden BB' mit dem Einheitskreis.



Schritt 3

Abbildung 4.4: Winkeldreiteilung

Beweis. Wir beginnen mit dem Beweis der Korrektheit.

Nach Konstruktion ist das Viereck B, Q, B', M in Abbildung (4.5) eine Raute, d.h. das Dreieck B, M, Q ist gleichschenklig, es folgt somit $\theta_1 = \theta_2$. Weiter gilt $\theta_2 = \theta_4$ und $\theta_3 = \theta_5$, da dies nur die gespiegelten Winkel an der Geraden QM sind. Der Punkt G wurde so konstruiert, dass er der Mittelpunkt von E und B ist, daher gilt auch $\theta_4 = \theta_5$. Zusammengefasst gilt somit: $\theta_1 = \theta_2 = \theta_3 = \theta_4 = \theta_5$. Da für den Winkel zwischen P, B und C die Gleichung $\varphi = \theta_1 + \theta_2 + \theta_3$ gilt, folgt $\varphi = 3 \cdot \theta_1$ und damit $\varphi/3 = \theta_1$.
Es bleibt noch zu zeigen, dass es reicht, Winkel zwischen 0 und $\pi/2$ zu betrachten, außerdem muss noch begründet werden, warum die Gerade in *Schritt 2* überhaupt existiert. Die Existenz folgt aus Bemerkung (4.2.1), da die Gerade BP und die Gerade GG' nicht parallel sind.

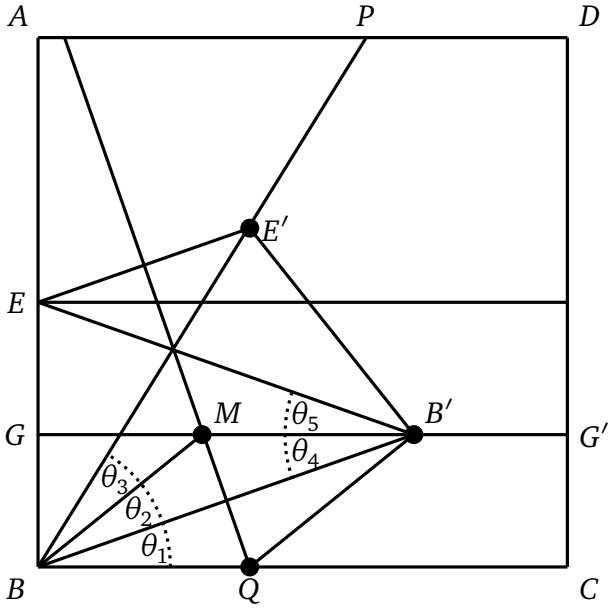


Abbildung 4.5: Winkeldreiteilung

Wegen

$$e^{i\pi/6} = \cos\left(\frac{\pi}{6}\right) + i\sin\left(\frac{\pi}{6}\right) = \frac{\sqrt{3}}{2} + \frac{i}{2} \in \mathscr{Z}(\{0,1\}) \subseteq \mathscr{O}(\{0,1,e^{i\varphi}\})$$

und $e^{i(\varphi+\pi/2)/3} = e^{i\varphi/3} \cdot e^{i\pi/6}$ reicht es tatsächlich, Winkel zwischen 0 und $\pi/2$ zu betrachten. □

Wir haben gesehen, dass wir Winkel mit Origami dreiteilen können. Es liegt daher auch nahe, dass mit Origami Kubikwurzeln von beliebigen komplexen Zahlen konstruiert werden können. Dazu zeigen wir dies im folgenden Satz zunächst für beliebige reelle Zahlen.

Satz 4.3.5. *Sei $r \in \mathcal{O}(K) \cap \mathbb{R}$, dann gilt $\sqrt[3]{r} \in \mathcal{O}(K) \cap \mathbb{R}$.*

Die folgende Beweisidee basiert auf der Tatsache, dass Axiom *(O6)* äquivalent zum Finden einer gemeinsamen Tangente zweier Parabeln ist, siehe [Ger08, Chapter 2, 8]. Wir wollen jedoch mit Rücksicht auf den Umfang dieser Arbeit einen eher auf linearer Algebra beruhenden Beweis führen.

Beweis. Sei $r \in \mathcal{O}(K) \cap \mathbb{R}$ und o.B.d.A. $r \neq 0$. Für diesen Beweis wollen wir $\mathbb{C}$ mit $\mathbb{R}^2$ identifizieren. Weiter seien die Punkte $p_1 := \left(\frac{r}{2}, 0\right)^T \in \mathbb{R}^2$ und $p_2 := \left(0, \frac{1}{2}\right)^T \in \mathbb{R}^2$ sowie die Geraden $l_1 : x = -\frac{r}{2}$ und $l_2 : y = -\frac{1}{2}$ gegeben. Da l_1 und l_2 nicht parallel sind, existiert nach Bemerkung (4.2.1) eine Gerade $s : y = c \cdot x + d$, die p_1 auf l_1 und p_2 auf l_2 spiegelt (s kann nicht parallel zur x- oder y-Achse sein, daher kann s wie angegeben dargestellt werden).
Unser Ziel ist es nun, die Koeffizienten c und d anzugeben.
Die Spiegelung an einer Geraden durch den Ursprung ist eine lineare Abbildung und wir können diese somit mit einer Matrix beschreiben, deren Darstellung man aus einem einfachen Basiswechsel erhält. Die Spiegelung des Punktes $p_1 = \left(\frac{r}{2}, 0\right)^T$ auf p_1' an der Geraden $s : y = c \cdot x + d$ entspricht daher der Gleichung

$$p_1' = \begin{pmatrix} 0 \\ d \end{pmatrix} + \frac{1}{1+c^2} \cdot \begin{pmatrix} 1-c^2 & 2c \\ 2c & c^2-1 \end{pmatrix} \cdot \left(\begin{pmatrix} \frac{r}{2} \\ 0 \end{pmatrix} - \begin{pmatrix} 0 \\ d \end{pmatrix} \right),$$

Analoges für p_2. Da p_1' auf l_1 und p_2' auf l_2 liegen sollen, erhalten wir die beiden Gleichungen

$$-\frac{r}{2} = \frac{1-c^2}{1+c^2} \cdot \frac{r}{2} - \frac{2cd}{1+c^2} \tag{1}$$

$$-\frac{1}{2} = (c^2-1)\left(\frac{1}{2} - d\right)\frac{1}{1+c^2} + d. \tag{2}$$

Gleichung *(1)* lässt sich nach d umformen und in *(2)* einsetzen, man erhält daher eine kubische Gleichung mit einer möglichen reellen Lösung für c und damit folglich auch für d:

$$c = -\sqrt[3]{r}$$
$$d = -\frac{r}{2\sqrt[3]{r}}$$

Der Schnittpunkt der Geraden s mit der y-Achse ist $(0, d)$, somit gilt $d \in \mathcal{O}(K)$. Da $\mathcal{O}(K)$ ein Körper ist, folgt daher aus $r \in \mathcal{O}(K)$ auch $\sqrt[3]{r} \in \mathcal{O}(K)$, was zu zeigen war. □

Im folgenden Korollar halten wir fest, dass wir mit obigen Überlegungen jede dritte Wurzel einer komplexen Zahl mittels Origami konstruieren können.

Korollar 4.3.6. *Aus $z \in \mathcal{O}(K)$ folgt $\sqrt[3]{z} \in \mathcal{O}(K)$ für jede komplexe dritte Wurzel von z.*

Beweis. Sei $z = r \cdot e^{i\varphi} \in \mathcal{O}(K)$, dann gilt $r, e^{i\varphi} \in \mathcal{Z}(K \cup \{z\}) \subseteq \mathcal{O}(K)$. Nach den Sätzen (4.3.3) und (4.3.5) folgt $\sqrt[3]{r}, e^{i\varphi/3+2i\pi j/3} \in \mathcal{O}(K)$ für $j = 0, 1, 2$. Aus der Körpereigenschaft von $\mathcal{O}(K)$ folgt somit $\sqrt[3]{z} \in \mathcal{O}(K)$ für jede dritte Wurzel von z. □

Lemma 4.3.7. *Der Körper $\mathcal{O}(K)$ aller aus $K \subseteq \mathbb{C}$ mit Origami konstruierbaren Zahlen ist der Durchschnitt aller Teilkörer L von $\mathbb{C}$ mit den folgenden Eigenschaften:*

(1) $K \subseteq L$

(2) $z \in L \Rightarrow \overline{z} \in L$

(3) $z \in L \Rightarrow \pm\sqrt{z} \in L$

(4) $z \in L \Rightarrow \sqrt[3]{z} \in L$ *(für jede komplexe dritte Wurzel von z)*

Beweis. Sei $M := \{L \subseteq \mathbb{C} | L$ ist ein Teilkörper von $\mathbb{C}$ der *(1)-(4)* erfüllt$\}$, wir wollen die Gleichheit

$$\mathcal{O}(K) = \bigcap_{L \in M} L =: \tilde{L}$$

wieder über Induktion zeigen, ähnlich dem Beweis von Lemma (3.3.3). Nach unseren Vorüberlegungen erfüllt der Körper $\mathcal{O}(K)$ alle vier Bedingungen, somit gilt $\tilde{L} \subseteq \mathcal{O}(K)$. Es bleibt somit noch die umgekehrte Inklusion zu zeigen. Wieder übertragen sich die Eigenschaften *(1)* bis *(4)* auf $\tilde{L}$ und es gilt

$$z \in \tilde{L} \Leftrightarrow \mathrm{Re}(z), \mathrm{Im}(z) \in \tilde{L}.$$

Wir wollen nun über vollständige Induktion zeigen, dass $K_n \cap \mathbb{C} \subseteq \tilde{L}$ gilt und alle Geraden in K_n mit Koeffizienten aus $\tilde{L}$ darstellbar sind, mit K_n aus der Definition von $\mathcal{O}(K)$. Für $n = 0$ gilt $K_0 = K \subseteq \tilde{L}$ nach *(1)* und K_0 enthält keine Gerade, somit gilt die Aussage für $n = 0$. Wir nehmen nun an, die Aussage gilt für ein $n \in \mathbb{N}_0$. Wie wir im Beweis von Lemma (3.3.3) gesehen haben, liegen Schnittpunkte von Geraden mit Koeffizienten in $\tilde{L}$ wieder in $\tilde{L}$, somit folgt $K_{n+1} \cap \mathbb{C} \subseteq \tilde{L}$. Um zu zeigen, dass alle aus K_n konstruierbaren Geraden Koeffizienten in $\tilde{L}$ besitzen, geben wir diese explizit an. Seien $p_1, p_2, l_1, l_2 \in K_n$ gegeben, wobei p_1, p_2 Punkte und $l_1(t) = a + tv$ und $l_2(t) = b + tw$ für $t \in \mathbb{R}$ Geraden sind. Wegen $|z| = \sqrt{\mathrm{Re}(z)^2 + \mathrm{Im}(z)^2} \in \tilde{L}$ für $z \in \tilde{L}$ können wir $|v| = |w| = 1$ annehmen. Nach Induktionsvoraussetzung liegen alle Koeffizienten in $\tilde{L}$. Die Geraden in *(O1)* bis *(O7)* haben dann folgende Gestalt:

- *(O1)*: $h(t) = p_1 + t(p_2 - p_1)$
- *(O2)*: $h(t) = \frac{p_1+p_2}{2} + t \cdot i(p_2 - p_1)$
- *(O3)*:
  - Falls l_1 und l_2 nicht parallel sind: $h(t) = s + t(v \pm w)$, wobei s den Schnittpunkt der beiden Geraden l_1 und l_2 bezeichnet, somit gilt auch $s \in \tilde{L}$.
  - Falls l_1 und l_2 parallel sind: $h(t) = \frac{a+b}{2} + tv$.
- *(O4)*: $h(t) = p_1 + t \cdot iv$
- *(O5)*: $h(t) = p_2 + t\left(p_2 - \frac{p_1+p_1'}{2}\right)$, wobei sich p_1' wie folgt berechnet: Die Spiegelung von p_1 an der gesuchten Gerade h soll auf der Gerade l_1 liegen, also muss für ein $s \in \mathbb{R}$ gelten:

  $$|l_1(s) - p_2|^2 = |p_2 - p_1|^2$$

  und $l_1(s) = p_1'$, wobei p_1' die Spiegelung von p_1 an h bezeichnet. Dies führt auf ein quadratisches Gleichungssystem der Form $xs^2 + ys + z = 0$ mit $x, y, z \in \tilde{L} \cap \mathbb{R}$ und $x \neq 0$, und da $\tilde{L}$ nach Voraussetzung abgeschlossen unter der Bildung von Quadratwurzeln ist, folgt aus der pq-Formel $s \in \tilde{L} \cap \mathbb{R}$ und damit $p_1' \in \tilde{L}$.

- *(O6)*: Dies ist der schwierigste Fall. Ist h parallel zur y-Achse, so hat h die Form $h(t) = \frac{p_1+p_1'}{2} + t \cdot i$, wobei p_1' den Schnittpunkt der Geraden l_1 mit $g(t) := p_1 + t$ beschreibt. Ist h nicht parallel zur y-Achse, so lässt sich h in der Form $h(t) = ui + t(1 + iq)$ für $u, q \in \mathbb{R}$ schreiben. Wir müssen nun $u, q \in \tilde{L} \cap \mathbb{R}$ zeigen. Wieder wollen wir kurzfristig $\mathbb{C}$ als $\mathbb{R}^2$ auffassen, als verkürzende Schreibweise benutzen wir $z_1 := \mathrm{Re}(z)$ bzw. $z_2 := \mathrm{Im}(z)$ für $z \in \mathbb{C}$. Da die Spiegelung von p_1 bzw. p_2 an h auf l_1 bzw. l_2 liegen soll, erhalten wir wieder folgende Gleichungen:

$$l_1(t) = \begin{pmatrix} 0 \\ u \end{pmatrix} + \frac{1}{1+q^2} \begin{pmatrix} 1-q^2 & 2q \\ 2q & q^2-1 \end{pmatrix} \left(\begin{pmatrix} p_{1,1} \\ p_{1,2} \end{pmatrix} - \begin{pmatrix} 0 \\ u \end{pmatrix} \right) \tag{1}$$

$$l_2(s) = \begin{pmatrix} 0 \\ u \end{pmatrix} + \frac{1}{1+q^2} \begin{pmatrix} 1-q^2 & 2q \\ 2q & q^2-1 \end{pmatrix} \left(\begin{pmatrix} p_{2,1} \\ p_{2,2} \end{pmatrix} - \begin{pmatrix} 0 \\ u \end{pmatrix} \right) \tag{2}$$

Daraus ergeben sich die vier Gleichungen

$$a_1 + t v_1 = \frac{1}{1+q^2} \left((1-q^2) p_{1,1} + 2q(p_{1,2} - u) \right) \tag{3}$$

$$a_2 + t v_2 = u + \frac{1}{1+q^2} \left(2q p_{1,1} + (q^2-1)(p_{1,2} - u) \right) \tag{4}$$

$$b_1 + s w_1 = \frac{1}{1+q^2} \left((1-q^2) p_{2,1} + 2q(p_{2,2} - u) \right) \tag{5}$$

$$b_2 + s w_2 = u + \frac{1}{1+q^2} \left(2q p_{2,1} + (q^2-1)(p_{2,2} - u) \right). \tag{6}$$

Da $v, w \neq 0$ (denn sonst wären l_1, l_2 keine Geraden), können wir o.B.d.A. $v_2, w_2 \neq 0$ annehmen. Durch Multiplizieren von *(4)* bzw. *(6)* mit $\frac{v_1}{v_2}$ bzw. $\frac{w_1}{w_2}$ und Subtrahieren von *(3)* bzw. *(5)* erhalten wir mit etwas Umformen

$$a_1 - a_2 \frac{v_1}{v_2} = \frac{1}{1+q^2} \left(p_{1,1} \left(1 - q^2 - 2q \frac{v_1}{v_2} \right) + p_{1,2} \left(2q - q^2 \frac{v_1}{v_2} + \frac{v_1}{v_2} \right) - 2u \left(q + \frac{v_1}{v_2} \right) \right) \tag{7}$$

$$b_1 - b_2 \frac{w_1}{w_2} = \frac{1}{1+q^2} \left(p_{2,1} \left(1 - q^2 - 2q \frac{w_1}{w_2} \right) + p_{2,2} \left(2q - q^2 \frac{w_1}{w_2} + \frac{w_1}{w_2} \right) - 2u \left(q + \frac{w_1}{w_2} \right) \right). \tag{8}$$

Gilt $q + \frac{v_1}{v_2} = 0$, so folgt $q \in \tilde{L}$ und wir können h auch schreiben als $h(t) = \frac{p_1+p_1'}{2} + t \begin{pmatrix} 1 \\ q \end{pmatrix}$, wobei $p_1' \in \tilde{L}$ den Schnittpunkt der Geraden $g(t) = p_1 + t \begin{pmatrix} q \\ -1 \end{pmatrix}$ mit l_1 beschreibt. Ist $q + \frac{v_1}{v_2} \neq 0$, so lässt sich *(7)* nach u umformen und in *(8)* einsetzen, wir erhalten dann eine Gleichung der Form $\alpha q^3 + \beta q^2 + \gamma q + \delta = 0$ mit $\alpha, \beta, \gamma, \delta \in \tilde{L} \cap \mathbb{R}$ in q. Mit der Cardanoschen Formel (2.3.11) erhalten wir $q \in \tilde{L} \cap \mathbb{R}$, da nach Voraussetzung $\tilde{L}$ abgeschlossen unter der Bildung von Quadrat- und Kubikwurzeln ist. Durch Umformen von *(7)* nach u erhalten wir damit auch $u \in \tilde{L} \cap \mathbb{R}$, was zu zeigen war.

- *(O7)*: $h(t) = \frac{p_1+p_1'}{2} + t \cdot iw$, wobei p_1' den Schnittpunkt von l_1 mit der Geraden $g(t) = p_1 + tw$ bezeichnet.

Damit haben wir die gewünschten Aussagen gezeigt und es gilt $\left(\bigcup_{n \in \mathbb{N}_0} K_n \right) \cap \mathbb{C} = \bigcup_{n \in \mathbb{N}_0} \left(K_n \cap \mathbb{C} \right) \subseteq \tilde{L}$. Daraus folgt die Gleichheit $\mathcal{O}(K) = \tilde{L}$. □

Wir wollen nun wieder ein Kriterium angeben, wann ein $z \in \mathbb{C}$ konstruierbar ist. Dies beweisen wir anschließend völlig analog zu den Theoremen (3.3.4) und (3.3.6).

Theorem 4.3.8. *Folgende Aussagen sind für $z \in \mathbb{C}$ äquivalent:*

i) $z \in \mathcal{O}(K)$

ii) Es existiert eine aufsteigende Kette von Körpererweiterungen $\mathbb{Q}(K \cup \overline{K}) = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_n \subseteq \mathbb{C}$ mit $z \in L_n$ und $[L_j : L_{j-1}] \in \{2, 3\}$ für alle $j = 1, ..., n$ (wieder bezeichnet $\overline{K} = \{\overline{k} \in \mathbb{C} | k \in K\}$).

iii) Es gibt eine Galoiserweiterung $L/\mathbb{Q}(K \cup \overline{K})$ mit $z \in L$ und $[L : \mathbb{Q}(K \cup \overline{K})] = 2^n 3^m$ mit $n, m \in \mathbb{N}_0$.

Beweis. Der Beweis verläuft vollkommen analog zu den Theoremen (3.3.4) und (3.3.6), wir gehen daher nur auf die Unterschiede und kleineren Details ein.

- "$i) \Rightarrow ii)$": Ist $M \subseteq \mathbb{C}$ die Menge aller Elemente, für die solch eine Körperkette existiert, so wollen wir wieder zeigen, dass M ein Körper ist, der die Eigenschaften *(1)* bis *(4)* aus Lemma (4.3.7) erfüllt. Dies lässt sich fast analog zu dem Fall mit Zirkel und Lineal beweisen, wir müssen nur die Bedingung "$a_{j+1}^2 \in L_0(a_1, ..., a_j)$" durch "$P(a_{j+1}) = 0$" für ein nicht konstantes Polynom $P(X) \in L_0(a_1, ..., a_j)[X]$ mit maximalem Grad drei" ersetzen. Wegen $[L_n(\sqrt[3]{z}) : L_n] \leq 3$ für $z \in L_n$ erfüllt M ebenso Eigenschaft *(4)*.
- "$i) \Leftarrow ii)$": Es gilt $L_0 = \mathbb{Q}(K \cup \overline{K}) \subseteq \mathcal{Z}(K) \subseteq \mathcal{O}(K)$. Sei $w \in L_1 \backslash L_0$, dann gibt es $a, b, c \in L_0$ mit entweder $w^3 + aw^2 + bw + c = 0$ oder $w^2 + aw + b = 0$. In beiden Fällen erhält man aus der Cardanoschen Formel (2.3.11) oder der pq-Formel $w \in \mathcal{O}(K)$. Wegen $[L_1 : L_0(w)][L_0(w) : L_0] = 3$ folgt $[L_1 : L_0(w)] = 1$ und somit $L_1 = L_0(w) \subseteq \mathcal{O}(K)$. Induktiv erhält man wieder $z \in L_n \subseteq \mathcal{O}(K)$.
- "$i) \Rightarrow iii)$": Auch hier müssen wir lediglich die Bedingung "$a_{j+1}^2 \in L_0(a_1, ..., a_j)$" durch "$P(a_{j+1}) = 0$ für ein nicht konstantes Polynom $P(X) \in L_0(a_1, ..., a_j)[X]$ mit maximalem Grad drei" ersetzen. Die Gruppe G_n aus dem entsprechenden Beweis ist dann wieder endlich und der Beweis für $\mathcal{O}(K)$ lässt sich durch simples Abändern weniger Details auf den Beweis für $\mathcal{Z}(K)$ zurückführen.
- "$i) \Leftarrow iii)$": Für die letzte Richtung benötigen wir das Resultat von Burnside (2.2.2), dass jede Gruppe der Ordnung $p^\alpha q^\beta$ auflösbar ist, für Primzahlen $p, q \in \mathbb{N}$. Daraus folgt der letzte Fall analog zu dem entsprechenden Fall mit Zirkel und Lineal.

□

Korollar 4.3.9. *Für $z \in \mathcal{O}(K)$ gilt $[Q_0(z) : Q_0] = 2^r 3^s$ für $r, s \in \mathbb{N}_0$ und $Q_0 := \mathbb{Q}(K \cup \overline{K})$.*

Beweis. Sei $z \in \mathcal{O}(K)$, dann existiert nach Theorem (4.3.8) eine Körperkette $\mathbb{Q}(K \cup \overline{K}) = L_0 \subseteq \cdots \subseteq L_n$ mit $[L_{j+1} : L_j] \in \{2, 3\}$. Daraus folgt $[L_n : L_0] = 2^k 3^t$ mit $k, t \in \mathbb{N}_0$ und damit $[L_0(z) : L_0] = 2^r 3^s$ für $r, s \in \mathbb{N}_0$. □

Dass alle Lösungen einer kubischen Gleichung $X^3 + aX^2 + bX + c = 0$ mit $a, b, c \in \mathcal{O}(K)$ Origami konstruierbar sind, ist nicht weiter verwunderlich, kennt man die Cardanosche Formel (2.3.11). Überraschenderweise lassen sich mit Origami jedoch auch alle Lösungen einer quartischen Gleichung $X^4 + aX^3 + bX^2 + cX + d = 0$ mit $a, b, c, d \in \mathcal{O}(K)$ mittels Origami konstruieren.

Korollar 4.3.10. *Alle komplexen Lösungen von $X^4 + aX^3 + bX^2 + cX + d = 0$ mit $a, b, c, d \in \mathcal{O}(K)$ sind mit Origami konstruierbar.*

Beweis. Sei $M := \{0, 1, a, b, c, d\}$ und L der Zerfällungskörper von $P(X) = X^4 + aX^3 + bX^2 + cX + d \in \mathbb{Q}(M \cup \overline{M})[X]$ in $\mathbb{C}$, d.h. $L = \mathbb{Q}(M \cup \overline{M})(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$, wobei $\alpha_1, ..., \alpha_4 \in \mathbb{C}$ die Nullstellen von $P(X)$ bezeichnen. Das Minimalpolynom jeder Nullstelle α_i über $\mathbb{Q}(M \cup \overline{M})(\alpha_1, ..., \alpha_{i-1})$ hat dabei höchstens Grad 4, weiter ist $L/\mathbb{Q}(M \cup \overline{M})$ eine Galoiserweiterung und somit gilt

$$[L : \mathbb{Q}(M \cup \overline{M})] = \underbrace{[L : \mathbb{Q}(M \cup \overline{M})(\alpha_1, \alpha_2, \alpha_3)]}_{\leq 4} \cdots \underbrace{[\mathbb{Q}(M \cup \overline{M})(\alpha_1) : \mathbb{Q}(M \cup \overline{M})]}_{\leq 4} = 2^r 3^s$$

für je ein $r, s \in \mathbb{N}_0$. Aus Theorem (4.3.8) folgt somit $\alpha_1, ..., \alpha_4 \in \mathcal{O}(M) \subseteq \mathcal{O}(K)$. □

4.4 Lösbarkeit der antiken Probleme mit Origami

Wie wir gesehen haben, lassen sich Winkel mit Origami dreiteilen und das delische Problem ist lösbar, d.h. $\sqrt[3]{2}$ ist konstruierbar. Wir halten dies im folgenden Satz fest und schließen diesen Abschnitt mit einer einfachen Konstruktion von $\sqrt[3]{2}$ mit Origami.

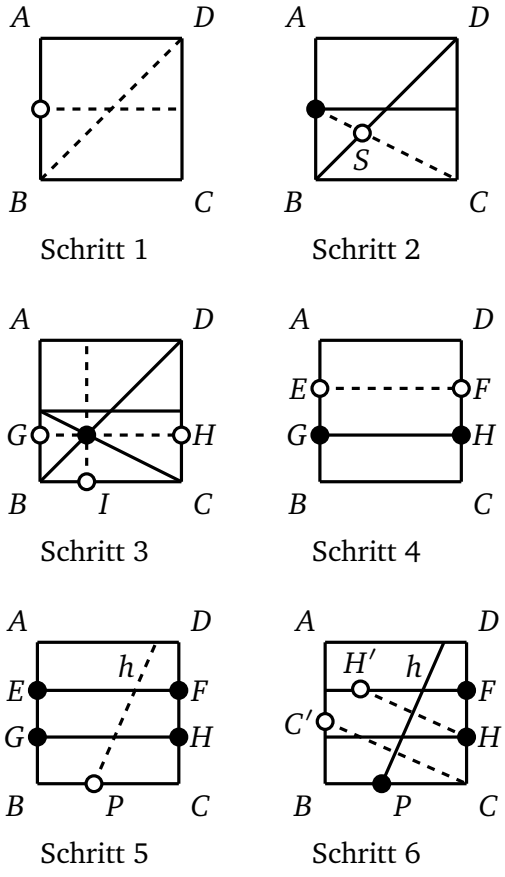
Satz 4.4.1. *Von den drei antiken Problemen ist nur die Quadratur des Kreises nicht mit Origami lösbar.*

Beweis. Es gilt $[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$, da π transzendent über $\mathbb{Q}$ ist, nach Korollar (4.3.9) folgt daher wieder $\pi \notin \mathcal{O}(\{0,1\})$. □

Die folgende Konstruktion ist zu finden in [Ger08, Chapter 2, 8] und wird Peter Messer zugeschrieben.

Konstruktion 4.4.2.

- Schritt 1: Wir falten die Mittelsenkrechte der Geraden AB sowie die Diagonale durch B und D. Der Schnittpunkt der Mittelsenkrechten mit der Gerade AB liegt natürlich mittig zwischen A und B.
- Schritt 2: Wir konstruieren die Gerade durch C und den Mittelpunkt von A und B. Den Schnittpunkt mit der Winkelhalbierenden aus Schritt 1 wollen wir kurzfristig mit S bezeichnen.
- Schritt 3: Mit S lassen sich die zu AB bzw. BC senkrechten Geraden durch S konstruieren. Die entsprechenden Schnittpunkte mit AB, BC und CD bezeichnen wir mit G, H und I, wie wir auch Abbildung (4.6) entnehmen können.
- Schritt 4: In Abbildung (4.6, Schritt 4) haben wir aus Gründen der Übersichtlichkeit die nicht mehr benötigten Geraden und Punkte entfernt. In diesem Schritt konstruieren wir die Mittelsenkrechte der Punkte A und G. Die neu entstandenen Schnittpunkte bezeichnen wir mit E und F.
- Schritt 5: Wir bilden die Gerade aus *(O6)*, indem wir C auf AB und H auf EF falten. Den Schnittpunkt mit BC bezeichnen wir mit P.
- Schritt 6: Wir bilden die zu h senkrechten Geraden durch C und H und bezeichnen die Schnittpunkte mit AB bzw. EF mit C' bzw. H'.



Schritt 1 Schritt 2 Schritt 3 Schritt 4 Schritt 5 Schritt 6

Abbildung 4.6: Konstruktion von $\sqrt[3]{2}$

Aus obiger Konstruktion folgt dann $\frac{|A-C'|}{|C'-B|} = \sqrt[3]{2}$.

Beweis. Wieder wählen wir o.B.d.A. die Punkte A, B, C, D als $i, 0, 1, 1+i \in \mathbb{C}$. Wir zeigen daher zuerst, dass $G = \frac{1}{3}i$ gilt. Die beiden Geraden l_1, l_2, wobei l_1 die Winkelhalbierende und l_2 die konstruierte Gerade in Schritt 2 beschreibt, sind gegeben durch $l_1(t) = t(1+i)$ sowie $l_2(s) = 1 + s(1 - \frac{1}{2}i)$. Durch lösen des linearen Gleichungssystems $l_1(t) = l_2(s)$ (Erinnerung: $t, s \in \mathbb{R}$) erhält man $S = \frac{1}{3}(1+i)$ und

somit $G = \frac{1}{3}i$, $E = \frac{2}{3}i$. Nun wollen wir $|A-C'| = \sqrt[3]{2} \cdot |C'-B|$ zeigen, dazu definieren wir $a := |A-C'|$, $b := |C'-B|$ und $c := |B-P|$, um die Übersichtlichkeit zu wahren. Wir halten zunächst fest, dass

$$a + b = 1 \tag{1}$$

gilt. Wegen $1-c = |P-C| = |P-C'|$ erhalten wir weiterhin $b^2 + c^2 = (1-c)^2$ und somit

$$c = \frac{1-b^2}{2}. \tag{2}$$

Da die Geraden $C'H'$ und $C'P$ senkrecht aufeinander stehen (denn dies sind nur die an h gespiegelten Geraden PC und HC), sind die Dreiecke mit den Eckpunkten E, C', H' und B, P, C' ähnlich und daher folgt

$$\frac{1/3}{a-1/3} = \frac{|C-H|}{|E-C'|} = \frac{|C'-H'|}{|E-C'|} = \frac{|C'-P|}{|B-P|} = \frac{1-c}{c}. \tag{3}$$

Durch Äquivalenzumformungen erhalten wir aus (3):

$$\begin{aligned}
\frac{1/3}{a-1/3} &= \frac{1-c}{c} \\
\frac{1}{3a-1} &\overset{(2)}{=} \frac{1+b^2}{1-b^2} \\
1-b^2 &= (1+b^2)(3a-1) \\
2 &= 3a(1+b^2) \\
2 &\overset{(1)}{=} 3(1-b)(1+b^2) \\
2 &= 2-2b^3+(1-3b+3b^2-b^3) \\
2b^3 &= (1-b)^3 \\
2b^3 &\overset{(1)}{=} a^3
\end{aligned}$$

Daraus folgt schließlich $\frac{a}{b} = \sqrt[3]{2}$. □

5 Vergleich von Origami mit Zirkel und Lineal mit Winkeldreiteilung

5.1 Erweiterungen von Zirkel und Lineal

Vergleichen wir Lemma (3.3.3) mit Lemma (4.3.7), so sehen wir, dass Origami die Konstruktionen mit Zirkel und Lineal lediglich um die Eigenschaft erweitert, komplexe dritte Wurzeln ziehen zu können. Wir können nun sicherlich die Frage stellen, ob und wie wir diese Erweiterung auch durch die Hinzunahme einer Operation zu den Konstruktionen mit Zirkel und Lineal erreichen können.

Eine Möglichkeit bietet z.B. ein markiertes Lineal, welches die Konstruktionen mit Zirkel und Lineal wie folgt erweitert: Sind zwei Geraden l_1, l_2 und ein Punkt P gegeben, dann ist die Gerade h durch P konstruierbar, sodass die beiden Schnittpunkte der Geraden h mit l_1 und l_2 genau eine Längeneinheit voneinander entfernt sind, siehe Abbildung (5.1).

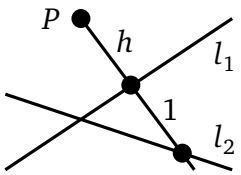


Abbildung 5.1: Markiertes Lineal

Es stellt sich nun die Frage, welcher Zusammenhang zwischen Origami und Zirkel und markiertem Lineal besteht. Tatsächlich stellt sich heraus, dass $\mathcal{O}(K)$ identisch mit der Menge der aus $K \subseteq \mathbb{C}$ mit Zirkel und markiertem Lineal konstruierbaren Zahlen ist ([Cox12, Theorem 10.3.11]).
Wir wollen uns nun jedoch der Frage widmen, ob die Hinzunahme der Winkeldreiteilung zu Zirkel und Lineal bereits genügt, um alle mit Origami konstruierbaren Punkte zu konstruieren. Wie wir gesehen haben, können wir das Konstruieren einer komplexen dritten Wurzel in zwei Teilprobleme zerlegen: Das Winkeldreiteilen und das Konstruieren einer reellen dritten Wurzel. Die Frage lautet also nun, ob man mit Winkeldreiteilung auch reelle dritte Wurzeln konstruieren kann. Im Folgenden wollen wir dies alles präzisieren und auf ein mathematisches Fundament stellen, um diese Frage beantworten zu können.

5.2 Zirkel und Lineal mit Winkeldreiteilung

Wir wollen die Konstruierbarkeit mit Zirkel und Lineal mit Winkeldreiteilung diesmal direkt über die algebraischen Eigenschaften definieren.

Definition 5.2.1. *Die Menge $\mathscr{Z}_D(K) \subseteq \mathbb{C}$ aller aus $K \subseteq \mathbb{C}$ (mit $0, 1 \in K$) mit Zirkel und Lineal mit Winkeldreiteilung konstruierbaren Zahlen ist definiert als der Durchschnitt aller Teilkörper L von $\mathbb{C}$ mit folgenden Eigenschaften:*

(1) $K \subseteq L$

(2) $z \in L \Rightarrow \overline{z} \in L$

(3) $z \in L \Rightarrow \pm\sqrt{z} \in L$

(4) $\sin(\theta) \in L \Rightarrow \sin\left(\frac{\theta}{3}\right) \in L$ *(mit* $\theta \in \mathbb{R}$*)*

Lemma 5.2.2. *Aus* $\sin(\theta) \in \mathscr{Z}_D(K)$ *folgt* $\sin\left(\theta + \frac{2\pi j}{3}\right) \in \mathscr{Z}_D(K)$ *für alle* $j = 0, 1, 2$.

Beweis. Mit den trigonometrischen Additionstheoremen erhalten wir

$$\sin\left(\theta + \frac{2\pi j}{3}\right) = \sin(\theta) \cdot \cos\left(\frac{2\pi j}{3}\right) + \cos(\theta) \cdot \sin\left(\frac{2\pi j}{3}\right)$$

für $j = 0, 1, 2$. Wegen $\cos(\theta) = \pm\sqrt{1 - \sin^2(\theta)}$ folgt aus Eigenschaft *(3)* auch $\cos(\theta) \in \mathscr{Z}_D(K)$. Aus einem geeigneten Tabellenwerk entnimmt man die Werte

$$\cos\left(\frac{2\pi j}{3}\right) \in \left\{1, -\frac{1}{2}\right\} \subseteq \mathscr{Z}_D(K) \text{ und } \sin\left(\frac{2\pi j}{3}\right) \in \left\{0, \pm\frac{\sqrt{3}}{2}\right\} \overset{(\star)}{\subseteq} \mathscr{Z}_D(K)$$

($(\star)$ folgt wieder aus *(3)*), daher folgt $\sin\left(\theta + \frac{2\pi j}{3}\right) \in \mathscr{Z}_D(K)$ für alle $j = 0, 1, 2$. □

Im nächsten Satz wollen wir wie üblich ein Kriterium angeben, wann ein gegebenes $z \in \mathbb{C}$ mit Zirkel und Lineal mit Winkeldreiteilung konstruierbar ist.

Satz 5.2.3. *Folgende Aussagen sind für* $z \in \mathbb{C}$ *äquivalent:*

i) $z \in \mathscr{Z}_D(K)$

ii) Es existiert eine aufsteigende Kette von Körpererweiterungen $\mathbb{Q}(K \cup \overline{K}) = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_n \subseteq \mathbb{C}$ *mit* $z \in L_n$ *und* $[L_j : L_{j-1}] \in \{2, 3\}$ *für alle* $j = 1, \ldots, n$ *(wieder bezeichnet* $\overline{K} = \{\overline{k} \in \mathbb{C} | k \in K\}$*), wobei* $L_j = L_{j-1}\left(\sin\left(\frac{\theta}{3}\right)\right)$ *im Fall* $[L_j : L_{j-1}] = 3$ *mit* $\sin(\theta) \in L_{j-1}$ *für ein* $\theta \in \mathbb{R}$ *ist.*

iii) Es existiert eine aufsteigende Kette von Körpererweiterungen $\mathbb{Q}(K \cup \overline{K}) = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_n \subseteq \mathbb{C}$ *mit* $z \in L_n$ *und* $[L_j : L_{j-1}] \in \{2, 3, 6\}$ *für alle* $j = 1, \ldots, n$ *(Wieder bezeichnet* $\overline{K} = \{\overline{k} \in \mathbb{C} | k \in K\}$*), wobei* L_j *im Fall* $[L_j : L_{j-1}] \in \{3, 6\}$ *der Zerfällungskörper des Polynoms* $4X^3 - 3X + \sin(\theta)$ *über* L_{j-1} *mit* $\sin(\theta) \in L_{j-1}$ *für ein* $\theta \in \mathbb{R}$ *ist.*

Beweis.

- "$i) \Rightarrow ii)$": Sei $M \subseteq \mathbb{C}$ wieder die Menge aller Elemente, für die solch eine Körperkette aus *ii)* existiert. Wir wollen die Definition (5.2.1) ausnutzen und zeigen, dass M ein Körper ist und alle Eigenschaften *(1)* bis *(4)* erfüllt. Die Körpereigenschaft und Eigenschaften *(1)* bis *(3)* folgen wieder vollkommen analog zum Beweis von Theorem (4.3.8), wir müssen also lediglich Eigenschaft *(4)* nachprüfen. Sei dazu $\sin(\theta) \in M$, d.h. es existiert eine Körperkette $\mathbb{Q}(K \cup \overline{K}) = L_0 \subseteq \cdots \subseteq L_n \subseteq \mathbb{C}$ mit den gewünschten Eigenschaften und $\sin(\theta) \in L_n$. Die Körpererweiterung L_{n+1}/L_n mit $L_{n+1} := L_n\left(\sin\left(\frac{\theta}{3}\right)\right)$ besitzt höchstens Grad 3, da eine Nullstelle des Polynoms $4X^3 - 3X + \sin(\theta) \in L_n[X]$ durch $\sin\left(\frac{\theta}{3}\right)$ gegeben ist. Somit folgt $\sin\left(\frac{\theta}{3}\right) \in L_{n+1} \subseteq M$ und daher haben wir $z \in \mathscr{Z}_D(K) \subseteq M$ gezeigt.

- "$ii) \Rightarrow iii)$": Dies folgt einfach, indem man alle Körpererweiterungen vom Grad 3 der Form $L_j = L_{j-1}\left(\sin\left(\frac{\theta}{3}\right)\right)$ durch "L_j ist der Zerfällungskörper des Polynoms $4X^3 - 3X + \sin(\theta)$ über L_{j-1} mit $\sin(\theta) \in L_{j-1}$ für ein $\theta \in \mathbb{R}$" ersetzt.

- "$iii) \Rightarrow i)$": Sei $\mathbb{Q}(K \cup \overline{K}) = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_n \subseteq \mathbb{C}$ eine Körperkette mit $z \in L_n$ und den gewünschten Eigenschaften. Es gilt $L_0 = \mathbb{Q}(K \cup \overline{K}) \subseteq \mathscr{Z}(K) \subseteq \mathscr{Z}_D(K)$. Induktiv zeigen wir nun $L_n \subseteq \mathscr{Z}_D(K)$. Sei $L_{n-1} \subseteq \mathscr{Z}_D(K)$ und $[L_n : L_{n-1}] = 2$, so folgt wie schon gesehen $L_n = L_{n-1}(\sqrt{c})$ für ein $c \in L_{n-1}$ und mit Eigenschaft *(3)* somit $L_n \subseteq \mathscr{Z}_D(K)$. Im Fall $[L_n : L_{n-1}] \in \{3, 6\}$ ist L_n der

Zerfällungskörper von $4X^3 - 3X + \sin(\theta)$ über L_{j-1} mit $\sin(\theta) \in L_{j-1}$ für ein $\theta \in \mathbb{R}$. Durch die trigonometrischen Additionstheoreme lässt sich folgende Identität nachprüfen:

$$4\sin^3\left(\frac{\theta}{3} + \frac{2\pi j}{3}\right) - 3\sin\left(\frac{\theta}{3} + \frac{2\pi j}{3}\right) + \sin(\theta) = 0$$

für alle $j = 0, 1, 2$. Daraus folgt

$$L_n = L_{n-1}\left(\sin\left(\frac{\theta}{3}\right), \sin\left(\frac{\theta}{3} + \frac{2\pi}{3}\right), \sin\left(\frac{\theta}{3} + \frac{4\pi}{3}\right)\right)$$

und aus Eigenschaft *(4)* und Lemma (5.2.2) daher auch $z \in L_n \subseteq \mathscr{Z}_D(K)$, was zu zeigen war.

□

Korollar 5.2.4. *Es gilt $\mathscr{Z}(K) \subseteq \mathscr{Z}_D(K) \subseteq \mathscr{O}(K)$.*

Beweis. Die erste Inklusion folgt direkt aus der Definition (5.2.1) von $\mathscr{Z}_D(K)$ und Lemma (3.3.3), die zweite Inklusion folgt aus obigem Satz (5.2.3) und Theorem (4.3.8). □

Wir wollen den vorigen Satz für reelle Zahlen, welche mit Zirkel und Lineal mit Winkeldreiteilung konstruierbar sind, noch etwas verschärfen, um die anfänglich gestellte Frage beantworten zu können.

Satz 5.2.5. *Falls $K \subseteq \mathbb{R}$ gilt, so sind folgende Aussagen für $z \in \mathbb{R}$ äquivalent:*

i) $z \in \mathscr{Z}_D(K)$

ii) Es existiert eine aufsteigende Kette von Körpererweiterungen $\mathbb{Q}(K) = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_n \subseteq \mathbb{R}$ mit $z \in L_n$ und $[L_j : L_{j-1}] \in \{2, 3, 6\}$ für alle $j = 1, ..., n$, wobei L_j im Fall $[L_j : L_{j-1}] \in \{3, 6\}$ der Zerfällungskörper des Polynoms $4X^3 - 3X + \sin(\theta)$ über L_{j-1} mit $\sin(\theta) \in L_{j-1}$ für ein $\theta \in \mathbb{R}$ ist.

Beweis.

"$i) \Leftarrow ii)$": Solch eine Körperkette erfüllt alle Voraussetzungen aus Satz (5.2.3), daher folgt $z \in \mathscr{Z}_D(K)$.

"$i) \Rightarrow ii)$": Sei $z \in \mathscr{Z}_D(K)$, dann existiert nach Satz (5.2.3) eine aufsteigende Kette von Körpererweiterungen $\mathbb{Q}(K) = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_n \subseteq \mathbb{C}$ mit $z \in L_n$ und $[L_j : L_{j-1}] \in \{2, 3, 6\}$ für alle $j = 1, ..., n$, sodass L_j im Fall $[L_j : L_{j-1}] \in \{3, 6\}$ der Zerfällungskörper des Polynoms $4X^3 - 3X + \sin(\theta)$ über L_{j-1} mit $\sin(\theta) \in L_{j-1}$ für ein $\theta \in \mathbb{R}$ ist.
Unser Ziel ist es nun, daraus eine reelle Körperkette mit den entsprechenden Eigenschaften zu konstruieren. Wir zeigen nun per Induktion: Für jedes $0 \leq k < n$ existiert eine Körperkette $L'_0 \subseteq \cdots L'_k \subseteq \mathbb{R}$ mit den Eigenschaften aus *ii)* und $L_k \subseteq L'_k(i)$. Wir definieren $L'_0 := L_0$, dann folgt trivialerweise $L_0 \subseteq L'_0(i)$. Sei nun $0 \leq k < n$ gegeben, sodass eine Körperkette $L'_0 \subseteq \cdots \subseteq L'_k \subseteq \mathbb{R}$ mit den Eigenschaften aus *ii)* und $L_k \subseteq L'_k(i)$ existiert. Um L'_{k+1} zu konstruieren, unterscheiden wir zwei Fälle:

- $[L_{k+1} : L_k] = 2$: In diesem Fall gilt $L_{k+1} = L_k(\sqrt{c})$ für ein $c \in L_k \subseteq L'_k(i)$. Wegen $|c|^2 = \mathrm{Re}(c)^2 + \mathrm{Im}(c)^2 \in L'_k$ ist $L'_{k,1}/L'_k$ mit $L'_{k,1} := L'_k(|c|) \subseteq \mathbb{R}$ höchstens eine quadratische Körpererweiterung. Weiter definieren wir $L'_{k,2} := L'_{k,1}(\sqrt{|c|}) \subseteq \mathbb{R}$, dies stellt ebenso eine quadratische Körpererweiterung dar. Wir können $c \in L'_k(i)$ auch schreiben als $c = |c| \cdot (\cos(\theta) + i\sin(\theta))$ mit $\theta \in \mathbb{R}$, wegen $c, |c| \in L'_{k,2}(i)$ folgt $\cos(\theta), \sin(\theta) \in L'_{k,2}$. Die Nullstellen des Polynoms

$$2X^2 - 1 - \cos(\theta) \in L'_{k,2}[X]$$

sind gegeben durch $\pm\cos\left(\frac{\theta}{2}\right) \in \mathbb{R}$, somit ist $L'_{k,3}/L'_{k,2}$ mit $L'_{k,3} := L'_{k,2}\left(\cos\left(\frac{\theta}{2}\right)\right) \subseteq \mathbb{R}$ wieder höchstens quadratisch. Mit $\sin\left(\frac{\theta}{2}\right) = \pm\sqrt{1 - \cos^2\left(\frac{\theta}{2}\right)}$ folgt, dass die Körpererweiterung $L'_{k+1}/L'_{k,3}$

mit $L'_{k+1} := L'_{k,3}\left(\sin\left(\frac{\theta}{2}\right)\right)$ ebenfalls quadratisch ist. Wegen $\sqrt{c} = \pm\sqrt{|c|}\cdot\left(\cos\left(\frac{\theta}{2}\right) + i\sin\left(\frac{\theta}{2}\right)\right)$ folgt $L_{k+1} = L_k(\sqrt{c}) \subseteq L'_{k+1}(i)$, somit ist die gesuchte Körperkette gegeben durch

$$L'_0 \subseteq \cdots \subseteq L'_k \subseteq L'_{k,1} \subseteq L'_{k,2} \subseteq L'_{k,3} \subseteq L'_{k+1} \subseteq \mathbb{R}.$$

- $[L_{k+1} : L_k] \in \{3, 6\}$: Hier entsteht L_{k+1} aus L_k durch Adjunktion der drei reellen Zahlen

$$\sin\left(\frac{\theta}{3}\right), \sin\left(\frac{\theta}{3} + \frac{2\pi}{3}\right), \sin\left(\frac{\theta}{3} + \frac{4\pi}{3}\right) \in \mathbb{R}$$

mit $\sin(\theta) \in L_k \cap \mathbb{R} \subseteq L'_k$. Definieren wir $L'_{k+1} := L'_k\left(\sin\left(\frac{\theta}{3}\right), \sin\left(\frac{\theta}{3} + \frac{2\pi}{3}\right), \sin\left(\frac{\theta}{3} + \frac{4\pi}{3}\right)\right)$, so ist L'_{k+1} der Zerfällungskörper von $4X^3 - 3X + \sin(\theta)$ über L'_k und es gilt

$$\begin{aligned} L'_{k+1}(i) &= L'_k\left(\sin\left(\frac{\theta}{3}\right), \sin\left(\frac{\theta}{3} + \frac{2\pi}{3}\right), \sin\left(\frac{\theta}{3} + \frac{4\pi}{3}\right)\right)(i) \\ &= \left(L'_k(i)\right)\left(\sin\left(\frac{\theta}{3}\right), \sin\left(\frac{\theta}{3} + \frac{2\pi}{3}\right), \sin\left(\frac{\theta}{3} + \frac{4\pi}{3}\right)\right) \\ &\supseteq \left(L_k\right)\left(\sin\left(\frac{\theta}{3}\right), \sin\left(\frac{\theta}{3} + \frac{2\pi}{3}\right), \sin\left(\frac{\theta}{3} + \frac{4\pi}{3}\right)\right) \\ &= L_{k+1}. \end{aligned}$$

Die gesuchte Körperkette ist damit gegeben durch

$$L'_0 \subseteq \cdots \subseteq L'_k \subseteq L'_{k+1} \subseteq \mathbb{R}.$$

Damit haben wir unsere Induktion abgeschlossen und wir sehen, dass für $z \in \mathscr{Z}_D(K) \cap \mathbb{R}$ wegen $z \in L_n \cap \mathbb{R} \subseteq L'_n$ die gewünschte reelle Körperkette mit den Eigenschaften aus *ii)* existiert. □

Korollar 5.2.6. *Es gilt* $\sqrt[3]{2} \notin \mathscr{Z}_D(\{0, 1\})$.

Beweis. Angenommen $\sqrt[3]{2} \in \mathscr{Z}_D(\{0, 1\}) \cap \mathbb{R}$, dann existiert nach Satz (5.2.5) eine aufsteigende Kette von Körpererweiterungen $\mathbb{Q}(K) = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_n \subseteq \mathbb{R}$ mit $\sqrt[3]{2} \in L_n$, $\sqrt[3]{2} \notin L_{n-1}$ und $[L_j : L_{j-1}] \in \{2, 3, 6\}$ für alle $j = 1, ..., n$, wobei L_j im Fall $[L_j : L_{j-1}] \in \{3, 6\}$ der Zerfällungskörper des Polynoms $4X^3 - 3X + \sin(\theta)$ über L_{j-1} mit $\sin(\theta) \in L_{j-1}$ für ein $\theta \in \mathbb{R}$ ist. Wieder unterscheiden wir zwei Fälle:

- $[L_n : L_{n-1}] = 2$: Da $\sqrt[3]{2}$ eine Nullstelle des Polynom $X^3 - 2 \in L_{n-1}[X]$ ist, der Körpergrad jedoch 2 ist, so darf das Polynom nicht irreduzibel sein, d.h. $X^3 - 2$ zerfällt über L_{n-1} in höchstens einen quadratischen Faktor und mindestens einen linearen Faktor, somit liegt mindestens eine Nullstelle von $X^3 - 2$ in L_{n-1}. Da die Nullstellen aber gegeben sind durch $\sqrt[3]{2}$, $\sqrt[3]{2}\zeta_3$, $\sqrt[3]{2}\zeta_3^2 \in \mathbb{C}$ mit $\zeta_3 = e^{2\pi i/3} \in \mathbb{C}\backslash\mathbb{R}$ und $L_{n-1} \subseteq \mathbb{R}$ gilt, folgt $\sqrt[3]{2} \in L_{n-1}$, im Widerspruch zu unserer Voraussetzung. Diesen Fall können wir somit ausschließen.

- $[L_n : L_{n-1}] \in \{3, 6\}$: Wie wir gesehen haben, muss $X^3 - 2$ irreduzibel in $L_{n-1}[X]$ sein. Da L_n der Zerfällungskörper von $4X^3 - 3X + \sin(\theta) \in L_{n-1}[X]$ über L_{n-1} ist, ist die Körpererweiterung L_n/L_{n-1} insbesondere normal. Nach Satz (2.3.3) folgt somit, da $X^3 - 2$ eine Nullstelle in L_n hat (nämlich $\sqrt[3]{2}$), dass bereits alle Nullstellen von $X^3 - 2$ in L_n liegen. Da aber zwei von drei Nullstellen echt komplex sind, L_n aber reell nach Voraussetzung war, haben wir den gewünschten Widerspruch und es folgt $\sqrt[3]{2} \notin \mathscr{Z}_D(\{0, 1\})$.

□

Wir haben damit gezeigt, dass Konstruierbarkeit mit Zirkel und Lineal mit Winkeldreiteilung nicht äquivalent zur Konstruierbarkeit mit Origami ist. Im Allgemeinen gilt somit $\mathscr{Z}(K) \subsetneq \mathscr{Z}_D(K) \subsetneq \mathscr{O}(K)$, da sich das delische Problem nicht mit Zirkel und Lineal mit Winkeldreiteilung lösen lässt.

6 Elliptische Kurven

6.1 Überblick

In diesem abschließenden Kapitel wollen wir vorangegangene Überlegungen und Resultate zur Konstruierbarkeit mit Origami auf elliptische Kurven anwenden, insbesondere werden wir Torsionspunkte der Ordnung zwei und drei betrachten. Hierzu müssen wir natürlich klären, was wir unter einer elliptischen Kurve verstehen wollen und wie wir mit ihr rechnen können, daher werden im folgenden Abschnitt die Grundlagen elliptischer Kurven zusammengefasst.

6.2 Grundlagen elliptischer Kurven

Definition 6.2.1 (Elliptische Kurve)**.** *Sei L ein Körper mit $char(L) \notin \{2,3\}$ und $a, b \in L$ gegeben. Die Nullstellenmenge von $f(X,Y) = Y^2 - X^3 - aX - b \in L[X,Y]$ in $L^2 \cup \{\infty\}$ bezeichnen wir mit $N_f(L) := \{(x,y) \in L^2 | y^2 = x^3 + ax + b\} \cup \{\infty\}$. Gilt $\Delta_f := 4a^3 + 27b^2 \neq 0$ (Δ_f heißt **Diskriminante** von f), so nennen wir $N_f(L)$ eine **elliptische Kurve** bezüglich f in L^2. Hierfür schreiben wir auch verkürzend $E_L : Y^2 = X^3 + aX + b$. Ist $K \subseteq L$ ein Teilkörper von L und $a, b \in K$, so sagen wir, dass die elliptische Kurve **über** K **definiert** ist. Wir schreiben weiter "P liegt auf der elliptischen Kurve $E_L : Y^2 = X^3 + aX + b$" für $P \in N_f(L)$.*

Diese eher simple Definition einer elliptischen Kurve ist für diese Arbeit vollkommen ausreichend, für eine ausführlichere und allgemeinere Definition einer elliptischen Kurve als projektive ebene Kurve verweisen wir auf [Wer02], [Sil09]. Die Hinzunahme von ∞ in der Definition von $N_f(L)$ ist nötig, da wir eine Verknüpfung auf elliptischen Kurven definieren wollen, bezüglich dieser eine gegebene elliptische Kurve eine abelsche Gruppe mit neutralem Element ∞ bildet. Wir geben im Folgenden erst eine anschauliche Motivation dieser Verknüpfung auf einer elliptischen Kurve in $\mathbb{R}^2$ an, ehe wir diese allgemein definieren.

Motivation 6.2.2 (Addition auf einer elliptischen Kurve)**.**

Sei $E_{\mathbb{R}} : Y^2 = X^3 + aX + b$ eine elliptische Kurve mit $a, b \in \mathbb{R}$ und seien weiter mit $P, Q \in \mathbb{R}^2 \cup \{\infty\}$ zwei Punkte auf dieser elliptischen Kurve gegeben. Gilt $P = \infty$, so definieren wir $P \oplus Q := Q$ (analog für $Q = \infty$). Sind $P, Q \neq \infty$ und $P \neq Q$, so schneidet die Gerade durch P und Q die Kurve in genau einem weiteren Punkt R (existiert kein Schnittpunkt, so sagt man, beide schneiden sich bei ∞). Wir definieren $P \oplus Q := \infty$, falls $R = \infty$, andernfalls definieren wir $P \oplus Q$ als den an der x-Achse gespiegelten Punkt von R. Der Fall $P = Q \neq \infty$ wird analog definiert, die Gerade durch P und Q wird lediglich durch die Tangente der Kurve am Punkt P ersetzt.

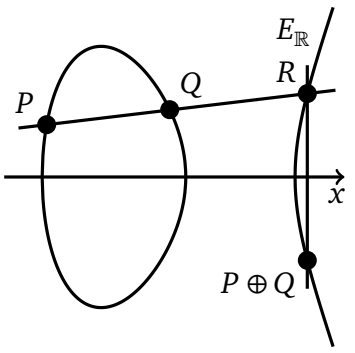


Abbildung 6.1: Addition auf einer elliptischen Kurve

Definition/Satz 6.2.3. *Sei wieder $E_L : Y^2 = X^3+aX+b$ eine elliptische Kurve mit $a, b \in L$ und seien weiter $P,Q \in N_f(L)$ zwei Punkte auf dieser elliptischen Kurve gegeben. Die Abbildung $\oplus : N_f(L)\times N_f(L) \to N_f(L)$, $(P,Q) \mapsto P \oplus Q$ mit*

$$P \oplus Q := \begin{cases} Q, & \text{falls } P = \infty \\ P, & \text{falls } Q = \infty \\ \infty, & \text{falls } P = (x,y) \text{ und } Q = (x,-y) \\ (x_3,y_3), & \text{falls } P = Q = (x,y) \text{ mit } y \neq 0 \\ (x_4,y_4), & \text{falls } P = (x_1,y_1),\ Q = (x_2,y_2) \text{ mit } x_1 \neq x_2 \end{cases}$$

und

$$(x_3,y_3) = (\lambda_1^2 - 2x,\ \lambda_1(x-x_3)-y) \qquad \lambda_1 = \frac{3x^2+a}{2y}$$
$$(x_4,y_4) = (\lambda_2^2 - x_1 - x_2,\ \lambda_2(x_1-x_4)-y_1) \qquad \lambda_2 = \frac{y_2-y_1}{x_2-x_1}$$

ist dann wohldefiniert und $\big(N_f(L), \oplus\big)$ bildet eine abelsche Gruppe mit neutralem Element ∞.

Für die obige Darstellung und den Beweis der Wohldefiniertheit siehe [Wer02, Satz 2.3.13+2.3.14], der Nachweis der Gruppeneigenschaften ist zu finden in [Sil09, III.2 Proposition 2.2].

Definition 6.2.4 (Torsionspunkte)**.** *Sei $E_L : Y^2 = X^3 + aX + b$ eine elliptische Kurve und P ein Punkt auf dieser elliptischen Kurve, dann bezeichnet $m \cdot P := \underbrace{P \oplus \ldots \oplus P}_{m-mal}$ die m-fache Addition von P, mit $m \in \mathbb{N}$.*
*Die Menge $E[m] := \{P \in N_f(L) | m \cdot P = \infty\}$ aller Punkte auf der elliptischen Kurve, deren Ordnung ein Teiler von $m \in \mathbb{N}$ ist, heißt **m-Torsionsgruppe**. Die m-Torsionsgruppe ist tatsächlich eine abelsche Gruppe bezüglich $\oplus$, wie man leicht nachrechnen kann. Die Elemente der m-Torsionsgruppe nennen wir **m-Torsionspunkte**.*

Definition 6.2.5. *Gilt $L = \mathbb{C}$ in Definition (6.2.1), so schreiben wir auch einfach $E : Y^2 = X^3 + aX + b$ für die elliptische Kurve bezüglich f in $\mathbb{C}^2$. Wir nennen $P \in \mathbb{C}^2 \cup \{\infty\}$ aus $K \subseteq \mathbb{C}$ **(Origami) konstruierbar**, falls $P = \infty$ gilt oder $P = (x,y)$ und x, y aus $K \subseteq \mathbb{C}$ (Origami) konstruierbar sind ($0, 1 \in K$ sei immer vorausgesetzt).*

6.3 Konstruierbarkeit der Torsionspunkte der Ordnung 2^n und $2^n \cdot 3$ mit Origami

Lemma 6.3.1. *Sei $E : Y^2 = X^3+aX+b$ eine elliptische Kurve in $\mathbb{C}^2$ definiert über $\mathcal{O}(K)$, d.h. $a, b \in \mathcal{O}(K)$. Dann sind alle 2- und 3-Torsionspunkte mit Origami konstruierbar.*

Die meiste Arbeit des Beweises haben wir schon in dem vorigen Kapitel geleistet, sodass dieser keinen allzu großen Aufwand erfordert.

Beweis. Sei $P \in E[2]$ ein Punkt auf der elliptischen Kurve gegeben. Ist $P = \infty$, so ist P nach Definition mit Origami konstruierbar. Andernfalls ergibt sich aus der Definition (6.2.3) der Verknüpfung an $P = (x,y)$ die Bedingung $y = 0$. Aus $0 = y^2 = x^3 + ax + b$ folgt dann nach Multiplikation mit x die Gleichung $0 = x^4 + ax^2 + bx$, somit ist x nach Korollar (4.3.10) ebenfalls mit Origami konstruierbar, wir haben damit gezeigt, dass alle 2-Torsionspunkte mit Origami konstruierbar sind.

Sei nun $P \in E[3]$ ein Punkt auf der gegebenen elliptischen Kurve. Wieder ist nur der Fall $P = (x, y) \neq \infty$ zu betrachten. Wegen $\infty = 3P = 2P \oplus P$ folgt mit $2P = (\tilde{x}, \tilde{y})$ die Bedingung $\tilde{x} = x$ und $\tilde{y} = -y$ mit $y \neq 0$. Es gilt

$$\begin{aligned}
\tilde{x} = x &\Leftrightarrow \left(\frac{3x^2 + a}{2y}\right)^2 - 2x = x \\
&\Leftrightarrow \frac{9x^4 + 6ax^2 + a^2}{4y^2} - 3x = 0 \\
&\Leftrightarrow 9x^4 + 6ax^2 + a^2 - 12y^2x = 0 \\
&\overset{(i)}{\Leftrightarrow} 3x^4 + 6ax^2 + 12bx - a^2 = 0,
\end{aligned}$$

wobei *(i)* aus $y^2 = x^3 + ax + b$ folgt, somit ist x wieder nach Korollar (4.3.10) mit Origami konstruierbar. Da $\mathcal{O}(K)$ abgeschlossen unter der Bildung komplexer Quadratwurzeln ist, folgt daher auch $y = \pm\sqrt{x^3 + ax + b} \in \mathcal{O}(K)$ und somit sind auch alle 3-Torsionspunkte mit Origami konstruierbar. □

Der obige Beweis scheitert im Allgemeinen bei der Betrachtung von Torsionspunkten höherer Ordnung, da wir die zu $m \cdot P = \infty$ (mit $P = (x, y)$) äquivalente Bedingung erhalten, dass $T(x) = 0$ für ein Polynom $T(X) \in \mathcal{O}(K)[X]$ mit Grad größer vier gilt. Gleichungen dieser Form lassen sich i.A. nicht mit Origami lösen, d.h. nicht alle Nullstellen eines Polynoms mit Grad ≥ 5 müssen Origami konstruierbar sein.
Wir geben noch zwei Eigenschaften Origami konstruierbarer Punkte auf elliptischen Kurven an.

Satz 6.3.2. *Sei $E : Y^2 = X^3 + aX + b$ eine elliptische Kurve in $\mathbb{C}^2$ definiert über $\mathcal{O}(K)$ und P, Q zwei Punkte auf dieser elliptischen Kurve mit $P = (x, y)$. Dann gilt:*

i) (x, y) ist Origami konstruierbar $\Leftrightarrow$ x oder y ist Origami konstruierbar.

ii) Sind P, Q Origami konstruierbar, so ist auch $P \oplus Q$ Origami konstruierbar.

Beweis.

i) "⇒": Ist (x, y) Origami konstruierbar, so sind nach Definition sogar x und y Origami konstruierbar, diese Richtung ist daher trivial.

"⇐": Ist x Origami konstruierbar, so gilt wegen $y = \pm\sqrt{x^3 + ax + b}$ auch $y \in \mathcal{O}(K)$, da $\mathcal{O}(K)$ abgeschlossen unter Bildung von Quadratwurzeln ist. Ist umgekehrt y Origami konstruierbar, so ist x als Nullstelle des Polynoms $X^3 + aX + b - y^2 \in \mathcal{O}(K)[X]$ ebenfalls Origami konstruierbar, wie wir schon mehrfach gesehen haben.

ii) Dies folgt direkt aus der Definition (6.2.3) der Addition auf einer elliptischen Kurve.

□

Satz 6.3.3. *Sei $E : Y^2 = X^3 + aX + b$ eine elliptische Kurve in $\mathbb{C}^2$ definiert über $\mathcal{O}(K)$. Dann sind alle Torsionspunkte in $E[2^n 3^m]$ mit $n \in \mathbb{N}_0$ und $m \in \{0, 1\}$ mit Origami aus $K \subseteq \mathbb{C}$ konstruierbar.*

Beweis. Die Aussage zeigen wir per Induktion nach $n \in \mathbb{N}_0$. Nach Lemma (6.3.1) sind Punkte auf der elliptischen Kurve der Ordnung 3^m mit $m \in \{0, 1\}$ Origami konstruierbar. Sei nun $P \in E[2^n 3^m]$ mit $n \in \mathbb{N}$ und $m \in \{0, 1\}$ gegeben. Gilt $2P = \infty$, so ist $P \in E[2]$ wieder nach Lemma (6.3.1) mit Origami konstruierbar. Sonst ist $2P = \tilde{P} \neq \infty$ ein Torsionspunkt in $E[2^{n-1} 3^m]$ und somit nach Induktionsvoraussetzung mit Origami konstruierbar. Mit $P = (x, y)$ und $\tilde{P} = (\tilde{x}, \tilde{y})$ erhalten wir die Gleichung

$$\begin{aligned}
& 2P = \tilde{P} \\
\Rightarrow\ & \frac{(3x^2 + a)^2}{4(x^3 + ax + b)} - 2x = \tilde{x} \\
\Rightarrow\ & x^4 - 4\tilde{x}x^3 - 2ax^2 - (8b + 4a\tilde{x})x + a^2 - 4\tilde{x}b = 0
\end{aligned}$$

mit Koeffizienten in $\mathcal{O}(K)$ nach Induktionsvoraussetzung. Aus Korollar (4.3.10) folgt $x \in \mathcal{O}(K)$ und damit aus Satz (6.3.2), dass $P \in E[2^n 3^m]$ mit Origami aus $K \subseteq \mathbb{C}$ konstruierbar ist, für alle $n \in \mathbb{N}_0$ und $m \in \{0, 1\}$. □

Abschließend wollen wir noch einen kurzen Ausblick geben. Wie wir gesehen haben, ist die Menge aller Origami konstruierbarer Punkte abgeschlossen unter der Verknüpfung auf einer elliptischen Kurve. Rationale Punkte auf elliptischen Kurven über $\mathbb{Q}$ spielen eine wichtige Rolle in der modernen Algebra, alle Problemstellungen lassen sich daher aufgrund dieser Eigenschaft auch bezüglich Origami konstruierbarer Punkte stellen, z.B. ob das Theorem von Mordell-Weil ([Cas95, 13, Theorem 1]) auch für Origami konstruierbare Punkte gilt. Eine Betrachtung dahingehend scheint sinnvoll, da sich mögliche Rückschlüsse auf rationale Punkte ziehen lassen könnten.

Literaturverzeichnis

[AL] Alperin, Roger C. ; Lang, Robert J.: One-, two, and multi-fold origami axioms. In: *In Proceedings of 4th International Conference on Origami, Science, Mathematics and Education. 4OSME, 2006. Caltech, Pasadena CA*

[Bos09] Bosch, Siegfried: *Algebra*. 7. Auflage. Berlin, Heidelberg : Springer, 2009. – ISBN 978–3–540–92811–9

[Bur04] Burnside, Williams: On groups of order $p^\alpha q^\beta$. In: *Proc.London Math. Soc.* 1 (1904), S. 388–392

[Cas95] Cassels, J.W.S.: *Lectures on Elliptic Curves*. Cambridge : Cambridge University Press, 1995. – ISBN 0–521–41517–9

[Cox12] Cox, David A.: *Galois Theory*. 2. Auflage. Hoboken, New Jersey : John Wiley and Sons, 2012. – ISBN 978–1–118–07205–9

[Fuc11] Fuchs, Clemens: Angle trisection with Origami and related topics. In: *Elemente der Mathematik* 66 (2011), S. 121–131

[Ger08] Geretschläger, Robert: *Geometric Origami*. Shipley : Arbelos, 2008. – ISBN 978–0–9–55–54–7

[JS06] Jantzen, Jens C. ; Schwermer, Joachim: *Algebra*. 2006. Berlin : Springer DE, 2006. – ISBN 978–3–540–21380–2

[KM13] Karpfinger, Christian ; Meyberg, Kurt: *Algebra - Gruppen - Ringe - Körper*. 3.Auflage. Berlin Heidelberg New York : Springer-Verlag, 2013. – ISBN 978–3827430113

[Lan] Lang, Robert J.: *Origami and Geometric Constructions*. `http://www.langorigami.com/science/math/hja/origami_constructions.pdf`, Abruf: 09. August. 2014

[Mey92] Meyers Konversations-Lexikon: *Quadratur des Zirkels*. `http://www.retrobibliothek.de/retrobib/seite.html?id=118999`. Version: 1885-1892, Abruf: 26. Juli. 2014

[Sil09] Silverman, Joseph H.: *Algebra*. 2. Auflage. Berlin, Heidelberg : Springer, 2009. – ISBN 978–0–387–09494–6

[Wer02] Werner, Annette: *Elliptische Kurven in der Kryptographie*. Berlin, Heidelberg : Springer, 2002. – ISBN 3–540–42518–7